Департамент профессионального образования Томской области
Областное государственное бюджетное профессиональное образовательное учреждение
Томский индустриальный техникум

СБОРНИК МАТЕРИАЛОВ
V ОТКРЫТОЙ НАУЧНО-ПРАКТИЧЕСКОЙ СТУДЕНЧЕСКОЙ КОНФЕРЕНЦИИ «БЕЗОПАСНОСТЬ ЧЕЛОВЕКА В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ»

30 ноября 2017 г.

г. Томск, 2017

В данном издании представлены работы V открытой научно-практической конференции «Безопасность человека в информационном пространстве».

Защита работ проходила по 4 секциям:

Секция 1. «Информационно-психологическая безопасность личности в информационном пространстве».

Секция 2. «Современные средства защиты «умных» объектов».

Секция 3. «Защита прав и интересов граждан в информационно-телекоммуникационных сетях».

Секция 4. «Информационная безопасность профессиональной деятельности в плакатах».

Сборник предназначен для студентов, преподавателей системы среднего профессионального образования, интересующихся проблемой формирования информационной культуры и безопасности пользователя в информационном пространстве.

Ответственность за содержание работы, грамматические и стилистические ошибки возлагается на авторов.

Оглавление

СЕКЦИЯ 1. «ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ»

БЕЗОПАСНОСТЬ ЛИЧНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Колесников Ярослав Романович
ОГБПОУ «Томский техникум информационных технологий»
Руководитель: Грушевский Юрий Викторович

С самых древних времён, обмен информацией был неотъемлемой частью взаимодействия между людьми. В контексте определённых тем люди делились-информировали друг друга новыми открытиями, представлениями, событиями.

Первым способом передачи информации стала речь. Позднее, в зависимости от уровня развития мышления, развивались способы передачи и сами типы информации, так как контекстов становилось всё больше – появилась письменность, позже книгопечатанье, а мы с вами находимся в периоде научно- технической революции.

Но как информация может повлиять на человека, а тем более на его сознание и личность?

Информация способна давать человеку много полезного, но информация может наносить вред, и этот вред может быть психологическим.

Прибегая к различным методам убеждения и внушения, информация может стать ключом к управлению сознанием и личностью.

Информацией можно эмоционально воздействовать на человека, а это наиболее эффективный способ управления.

Информационный шум

В наше время можно заметить, что многие люди не очень хорошо разбираются в теме, по которой активно дискутируют. Они утверждают, что знают

многое по этому вопросу, но почему-то во время беседы показывают поверхностные или обрывочные знания. Люди в большинстве своём не понимают причинно-следственных связей в огромном объёме получаемой информации.

Сейчас происходит информационная революция, информация перестала быть недоступной, ценной и фундаментальной. Раньше, чтобы получить ценную книгу, необходимо было отстоять в очереди или достать её через десятые руки — такое издание было на вес золота. Специальных обучающих курсов для обычных людей практически не было. Рецепты приготовления еды передавались по наследству, а к советам старших прислушивались как к самому важному.

Теперь в один клик можно изучить Вселенную, понять правила ведения бизнеса, узнать 25 рецептов салата оливье, осилить технологию монтажа гипсокартона. Приправьте это сверху блогами, лайками, цитатами, почтой, сериалами и самым вкусным с ТВ.

Раньше ценилось умение воспринимать информацию, усваивать, а главное, использовать её. Сейчас всё немного по-другому: надо уметь упорядочивать и фильтровать потоки информации, а главным становится её поиск. Человеческий мозг не может уже усвоить всю информацию, он просто помнит, где она и как хранится. Он уже не хочет запоминать причинно-следственные связи. Мозг превращается в быстрый компьютер.

Человек теперь не хочет анализировать и воспринимать информацию, он начинает привыкать к простому инфопотоку, не вникая, что там (вспомните чтение по диагонали). Но в этом и кроется главная опасность: вырабатывается зависимость от информации. Курсы, блоги, статьи, видео, фотографии — на это тратится много энергии и времени, а толку на выходе зачастую ноль.

Источники шума

1. Телевидение
2. Интернет
3. Радио
4. Газета

5. Реклама
6. Информационный фон

Это произошло из-за больших объёмов информации и сложности её обработки. Но, к сожалению, вместо решения проблемы при помощи этого мощного инструмента некоторые люди способны затуманивать и изменять сознание людей, создавать в голове кашу, приучить человека мыслить как машина.

Управление сознанием и личностью человека средствами информационных технологий

Если вместе с информационным шумом использовать методы психологического воздействия, то можно управлять не только одним человеком, а целой группой, страной, планетой. При помощи интернета и различных устройств это можно делать на расстоянии.

Но для чего это нужно?

Ведение информационных войн

Информационная война - одно из страшных явлений нашего мира. Это противоборство в информационном пространстве с целью достижения информационного, психологического и идеологического превосходства. Разделяется на два вида:

- **Информационная война при военных действиях.**

Данные технологии использовались в 1960-е годы и в течение всего периода холодной войны. Но на самом деле это использовалось более тысячи лет назад. Вся суть - разрознить между собой людей противника, посеять смуту, хаос, растлить, навязать идеологию. При помощи средств массовой информации, через медиа-контент: новости, музыка, фильмы, видео-блоги, сайты, телепередачи.

В конце концов у людей противника изменяется сознание и личность.

- **Информационная война внутри страны.**

Внутри страны это работает примерно так же, как и при военных действиях, только в ней участвуют правительство, крупные/некрупные организации, люди, проживающие в этой стране. Со стороны государства или страны

информационная война идёт против населения, чтобы контролировать общественное мнение, действия, потребности людей.

Организации могу работать против государства или наоборот, но преследуют они примерно те же цели, что государство или страна.

Население по большей части является жертвой и разносчиками. Но внутри населения есть сообщества, которые также сражаются на информационном побоище. Среди них люди, отстаивающие собственные идеи, и люди, отстаивающие чужие идеи.

По большей части эта война влияет на новые поколения. В том числе и поколение моего возраста. Практически весь медиа-контент пропитан нелепостью, двусмыслием, растлением. То, что происходит на YouTube и других видео-хостинговых сервисах, разрушает все этические и моральные устои нашей русской культуры, то же самое происходит и в официальных новостях. Видеоблогеры, группы в социальных сетях, различные информационные сайты несут в себе пропаганду организаций или идеологии других стран, неадекватный растлевающий контент, который принимает большинство. Маленькие детишки уже с самого детства становятся участниками всей этой паутины. Их личность будет растлена и сознание тоже, помимо того, что они будут управляемы, они будут агитировать других, потому что они будут так воспитаны.

Это основные принципы воздействия на людей в информационном пространстве. Легко управлять той культурой, которая лишается своей идеи и ценностей. Чтобы убедиться в том, что всё плохо, достаточно зайти на YouTube во вкладку “ В тренде” и посмотреть количество просмотров.

Как защитить свою личность в информационном пространстве?

Моё мнение по этому поводу довольно простое. Я считаю, что это поможет не только обезопасить личность и сознание, но и развитию нашей страны в информационном пространстве:

- Сократить информационный шум за счёт сокращения информации, получаемой в социальных сетях, почте, смартфоне.
- Изучать историю и не забывать наших предков.

- Найти себя в культуре, искусстве, науке.
- Сомневаться в авторитетах и задавать вопросы.

Список используемых источников:

1. https://lifehacker.ru/2016/01/15/informatsionnyj-shum/
2. https://militaryarms.ru/novye-texnologii/informazionnie-voiny/

НАША ЖИЗНЬ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Чердынцев Вадим Александрович
ОГБПОУ «Томский техникум информационных технологий»
Руководитель: Кабикова Алина Владимировна

Мое понимание термина «информационная безопасность» очень простое – это защита того, что не для всех предназначено.

Объект данной исследовательской работы – психология и тело человека, а также реализация человека в информационном обществе.

Цель работы: рассмотреть на примере своей и жизни общества тему «Безопасность человека в информационном пространстве».

Для реализации цели необходимо решить ряд задач:

- найти и обработать информацию по данной теме, как в настоящее время, так и в будущем;
- рассмотреть вопросы безопасности личной информации, привести примеры нового оборудования для информационной безопасности.

Выдвинуто предположение о том, что тело и разум в естественном виде человека не сможет принять новых технологий в будущем, а вот информационная безопасность человека станет намного лучше и проще.

В работах фантастов, которые только представляли себе будущее со сверхтехнологиями, часто рассматривалась позиция данных. Допустим, сейчас не 2017 год, а 3017 год. Современное представление человека будет уже мало похоже на что-то природное, и восприятие жизни явно изменит свой вид. Я сам учусь на программиста, и лишь отчасти меня интересует данная тема в таком разрезе: как бы я защитил свои данные?

Сейчас есть разные представления, кто-то уверен, что мы в матрице живём? Может, мы и есть боги? Может, эта жизнь уже была, и в ней все мои действия запланированы. Технологии бурно развиваются без оглядки на свои старые модели. Мы идём к тому, что скоро будем вживлять имплантаты, которые дадут нам лучше увидеть и почувствовать этот мир. И все бы ничего, но

мы так тесно связаны с нашей природой. Наша сущность стремится к дальнейшей эволюции, при этом ведет себя, судя по повадкам, как вирус. Почему именно вирус? Он точно также потребляет, как и мы, чтобы жить, а все остальное находит свои пределы и гармонизирует в отличие от нас.

При разговоре с учителем услышал от него свои слова, которые меня поразили. Был разговор про технику, которая бешено развивается, и когда-то на уроке биологии уже писал такую мысль: «Какой смысл развивать технологии, если мы не сможем их в том виде, в котором мы существуем, принять», тогда я мало уделил этому моменту значение, от меня лишь требовалось сдать домашнюю работу. И когда мы начали говорить о будущих технологиях, я вспомнил свои слова.

Однажды, как предположили мы с вами, в 3017 году изменится мир и человек из 2017 года, скорее всего, не будет рад этому. Почему не рад? Все опять же сводится к нашей психологии. Наш организм проще описать на программирование. У нас есть тело, справочник, команды, которые обязаны сделать, источники питания, разум выступает как камера самая обыкновенная, а уже мозг является студией для обработки (вырезки определённых воспоминаний), и также все мы обладаем чувствами, которые отличают нас от железа компьютера. Я больше приверженец теории, что все наши эмоции - это часть какого-то уравнения, которые стремится к гармонии.

Не зря начал наш разговор про внешний и внутренний мир человека. В 2017 году я понял, что моя бабушка, когда рассказывал ей про искусственный интеллект и даже включил видео, удивилась - как это? Устройство само общается с человеком и тут начинается хаос, как? У него есть душа? Я из поколения «нулевых», с самого детства за компьютером, и мне, как правило, это просто понять, что есть у него структура на языке программирования, который описывает выполнение команд. Она не смогла этого понять и сколько бы ни объяснял ей это, очень тяжело для неё, и тут возникла идея. Заключается она в такой истине простой: однажды и я буду чего-то не понимать!

Есть еще одно главное условие и отличие нас от компьютера. Наша память – это устройство, которое постоянно записывает информацию, перезаписывает основные массы знаний, полученных за всю нашу жизнь. Я хотел бы на примере объяснить, что память, которая используется ежедневно, это очень сложный механизм. Самое главное, что подобно кассете обычной или DVD-диску каждый день мы можем перезаписать, т.е. значит, забыть, потому, как это является ежедневным нашим исполнением обязанностей своих. Мы учимся, познаём себя и окружающий мир, и пределу этому нет. Но от проблемы потери и перезаписи информации мы так и не сможем избавиться. И результат моей любимой бабушки это показывает и однажды и на мне покажет. Суть такова: мы не можем переучиться, имея уже какие-то знания, которые используются в обиходе. Пример: попробуйте есть не с правой руки (для левши), а с левой (для правши) и поймете, что это не так и легко. У меня, когда-то мечта была в детстве, весьма странная. Лично я не стеснялся общества, но всегда боялся говорить с другими, мне было как-то неудобно. Сейчас этого нет, и мечта была следующей - запомнить всю свою жизнь. До 11 лет я все помнил, начиная с осознания себя самого. А вот, допустим, сейчас, я даже не могу вспомнить некоторые моменты, а если и вспоминаю, то каким-то неожиданным образом. Также мои моменты памяти очень странно завязаны. Я привык всегда, чтобы ни делал, слушать музыку, кроме моментов, когда мне что-то рассказывают, или я что-то делаю серьёзное. Самое главное, музыка как раз служит связующим звеном памяти. Уже слабо помню момент так же, как и песни, но такой парадокс: услышу музыку, которую когда-то слышал в 2007 году, а, может, в другом году, резко вспоминаю моменты, которые, по сути, просто так нельзя вспомнить. Можно сказать, расставляю флажки в своей памяти при помощи композиций. Все то, о чем мы говорили, касается личной информации, и я с вами поделился частью себя.

А что насчет личной информации, опять ссылаюсь на 3017 год. В нём очень важную роль играет ваше душевное состояние, как раз та проблематика, связывающая нас с природой, с нашей сущностью. Вы только представьте: уже

сейчас можно ставить весьма способные имплантаты и вживлять чипы для коммуникаций в быту. Технология – это вещь, которая проникает в нас и меняет наше сознание. Самая важная черта сознания, присущая всем, это деление поступков на добро и зло. А когда мы будем частью машины, которая улучшит нашу жизнь? Скажем ли мы, что тогда и сейчас все также останется. Многие люди из 2017 года даже будут не готовы осознавать тех простых основ добра и зла, которые уже будут в другой форме. В фильме «Призрак» был момент, как робот подключился к мозгу человека и копался в его личных данных, при этом у него стояли защиты на взлом, в итоге после этого, как забрали все, он умер. Это сравнение показывает будущее, хранение информации всегда будет в нас, т.е. внутри.

Свою статью не зря начал про внешние, внутренние качества человека и его сознание. Сама основа безопасности отвечает на тот вопрос: нужно защитить информацию от проникновения туда третьих лиц. Также есть фильм «Начало», там со снами связан был сюжет, что нужный им герой обладал информацией, и они его усыпили и пытались внушить ему идею, т.е. проникли в сознание, не украли, но изменили ход его жизни. Наша жизнь одна, и про память тоже не напрасно были сказаны слова. Смысл жизнь добиться того, что хотел, передать свою функцию своему потомству, как и знания, и уйти в неизвестность. Это лишь образное описание жизни и, конечно, так в одном предложении нельзя описать всю жизнь, что проживёт человек. В будущем уверен, что будет защита связана с сознанием человека или то, что от него останется от сторонних угроз.

Сейчас же в 2017 году ведутся постоянные работы как в сфере IT, так и в сфере военной организации, два направления идут на тесную связь. А откуда же появляется работа самой информации? Мы все также источниками и служим, мы получаем, раздаём и стираем информацию. Поэтому у специалистов, связанных с информационной безопасностью всегда будет работа в любое время. Информации, которая всегда появляется из общества, не то чтобы нужен контроль, ей нужен, скорее, тот, кто будет контролировать какие-либо

нарушения и несправедливость людей по отношению друг к другу. Мы как по библейской истории «Рождения света за 7 дней» поддаёмся на искушения, страхи, и удовольствие. Порой вещи, которые можем сделать, не контролируемы и чаще всего касаются других людей, ибо все мы живём на одной планете.

Из сериала «Викинги» узнал одну мудрость очень интересную [1]. Викинг по имени Рагнар Лотброк и король Экбрет размышляли о своей вере. В итоге дискуссии пришли к мнению о том, что Вальхала или Рай бессмысленны. Это лишь часть власти и контроля, которые позволяют человеку жить правильно. Чаще всего это та вера, за которую он молит свои решения, которые боится принять. Не бросайтесь сразу отказываться от веры, ибо это лишь мое мнение. Верить – это не значит отдать все. Само понятие веры является не только верой в богов или другие ценности вашей жизни, а вообще смыслом, который не требует объяснения. Если не верить ни во что, то можно и с ума сойти. И вот можно теперь понять тех людей из 2017 года, т.е. нас, и людей из 3017 года, когда все основы уже изменились полностью.

Часто люблю размышлять о нашем мире. То, что будет в будущем неописуемо для нас с вами, лишь можем вообразить, как бы это было проще для нас. Люди так далеки вообще еще от тех истин, которые не подадутся нашему сознанию. И как бы странно ни звучала моя статья о том - вот это все информационная безопасность? Да, это все! Все, что есть, оно всегда очень простое и, как правило, всегда рядом. Вопрос один: сможем ли мы сохранить себя, свою душу именно такой, какую имеем сейчас.

Все говорим о технике, если вернутся в наш 2017 год, то сейчас лицензионное программное обеспечение широкое значение получило у общества. Компания INTEL, разработчики операционной системы Windows, постоянно работают над улучшением системы. Первое, что заметил в 10 версии, к примеру, они пытаются сделать адаптивную платформу для мобильных и ПК-техники оболочку, которая бы позволяла работать с ними параллельно. Пример этой реализации можно представить, как через программу SideSync, связывающую планшет и компьютер в одну рабочую среду (рисунок 1).

Рисунок 1 – Рабочая среда

Это рабочая среда в компьютере и в планшете. Так вот, INTEL хочет сделать, например, свой Windows, одну систему и чтобы это была не сторонняя программа для объединения всех программ. Сейчас уже все говорят про обучающие платформы для общества, которые будут держать, какие-то организации, а мы будем подключаться как пользователи.

К чему эти сведения про INTEL и про объединение технологий? К тому, что тема у нас не просто безопасность, а связана она с информационными технологиями. И,таким образом, как думаете, если загнать всех пользователей Windows под одну платформу, что будет? Правильнее сказать, будет глобальная новая система Интернета, в этом есть плюсы и минусы. Естественно плюсы заключаются в том, что это будет удобно, быстро, и это не будет как раньше Интернет – мусорной свалкой ссылок, а минусы данной технологии – это как раз контроль, который обеспечивает порядок. Вроде, что такого? Я же выступал за контроль, чтобы он был? Но настаивал на том мнении, которое за те неравенства между людьми, в которых есть тот, у кого правда, и у кого ложь. А эта система будет хуже только в одном, если переведут все продукты на неё. Это будет явно тотальный контроль, и лишь мнимая черта выбора пользователя. Из плюсов еще это устранит всех нелицензионных обладателей программ. Соответственно, когда введут общую платформу для образования, медицины, военной структуры, науки, эти все вещи станут легко проверяемыми, и когда будут устанавливать справедливость и равенство. Как говорят еще, что равенство и справедливость, тоже разные понятия.

Вернемся к религии и власти, которую постоянно получают люди, которую не в силах отдать народу неправильное государство, собственно, мы пока на данном этапе. Не могу судить точно, правильно это или нет, лишь фантазия о том, что будет дальше с нашим телом и разумом.

Человек, у которого была записана память с его добром и злом, с его мамой и папой, с его началом жизни, тяжелой или лёгкой, неважно это все. Единственная истина, которая касается сознания про суждения друг о друге, это момент. Порой ведь достаточно взглянуть, и ты уже любишь человека, казалось бы, за что? За тот трехсекундный невинный взгляд? Нет, за тот промежуток времени? Нет, но во множестве романов и пьес все зовут это любовью. А вы знаете, как над любимым человеком вершить суд? Допустим страшную ситуацию вам нужно выбрать одного из своих родителей, которые вас оба любят, и встать на сторону одного из них на расстрел, вот вам выпала такая ноша, как вы будете судить? Ясно, что вы промолчите, ибо это святое, это нельзя выбрать, это ваши создатели для вас, они не хуже богов родных. Информационная безопасность – вещь, которая непосредственно связана с нами с самой сутью человеческой натуры, которая указывает нам, что эмоции человека и его поведение часто служат той вещью, когда мы наиболее становимся уязвимы для злоумышленника. Поэтому ,наверное, это будет самый большой минус всех учителей в мире, вы не можете оценить знания того или иного ученика, к примеру, на 4 и 5?! Если бы это был тест, который сам составил бы вопросы, например, нейронная сеть, по тому или иному разделу. Вы рассказываете ему, и он вас оценивает, вот это было бы правильно, ведь машине не нужны чувства для определения знаний человека, она лишь получает ответы, из которых и делает вывод, знает или нет. И часто учиться только на «5» не всегда выгодно. Это постоянное недосыпание, плюс еще трата полного личного времени, которое в итоге отразится на поведении человека в будущем.

Информационная безопасность ведёт к единству всех, и всегда можно найти минусы и плюсы. Работа сама нацелена на справедливость между людьми. Ведь если мы не будем уважать друг друга, если мы забудем простые

истины: «не убей» или «не укради» - разве мы будем при смене сознания в 3017 году звать себя людьми? Все наши поступки и действия порой решают не только нашу судьбу, но и судьбу дорогих нам людей.

В результате событий, которые описаны из реальной и предполагаемой жизни 2017 и 3017 года можно утверждать, что сформулированная ранее нами гипотеза подтверждена и служит доказательством, что тело и разум в естественном виде человека не сможет принять новых технологий в будущем, а вот информационная безопасность человека станет намного лучше и проще.

Поэтому хочу завершить свою работу такой цитатой, который сказал самый добрый актёр Евгений Леонов: «Я теперь стал верить ну не в бога, я так переделаться быстро не могу, а в то, что выше закона может быть любовь, выше права милость, выше справедливости может быть прощение. Мне кажется этого достаточно, чтобы жить». [2]

Список используемых источников:

1. https://www.youtube.com/watch?time_continue=56&v=-eOYhBaFj44.
2. https://www.youtube.com/watch?v=ZZM2rVZoN74

ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТА

Муравьев Роман Вячеславович
ОГБПОУ «Томский политехнический техникум»
Руководитель: Самсонова Ольга Викторовна

Цель работы: Провести исследование по теме «Правила безопасного использования Интернета»

Актуальность: Информационное пространство оказывает беспрецедентное влияние на безопасность личности и общества. В XXI веке средства массовой информации присутствуют повсюду, превращая каждое событие в товар, делая из него зрелищный спектакль, часто напоминающий фильм ужасов, что, казалось бы, идет вразрез с их основной функцией — предоставлять аудитории объективную информацию о происходящем.

Задачи:

1. Рассмотреть угрозы информационной безопасности в обществе.
2. Определить способы психологической защиты.
3. Создать буклет-памятку интернет-пользователя.

Методы:

1. Изучение литературы.
2. Аналитическая деятельность.

Введение

В отношении человека государство должно обеспечивать информационно-психологическую безопасность.

Информационно-психологическая безопасность - состояние защищенности отдельных лиц и (или) групп лиц от негативных информационно-психологических воздействий и связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере. Основными принципами обеспечения информационно-психологической безопасности являются:

- адекватность мер безопасности существующим угрозам;

- государственная монополия на разработку и производство специальных средств информационно-психологического воздействия;
- сочетание централизованного управления силами и средствами обеспечения информационно-психологической безопасности с передачей в соответствии с федеральным устройством России части полномочий в этой области органам государственной власти субъектов РФ и органам местного самоуправления;
- гласность и гражданский контроль за обеспечением информационно-психологической безопасности;
- обязательность участия общественных организаций в деятельности по обеспечению информационно-психологической безопасности.

Объекты угроз и их источники

К основным угрозам информационно-психологической безопасности относится возможность наступления негативных последствий для субъектов, подвергающихся информационно-психологическому воздействию, которые могут выражаться в следующих формах:

- причинение вреда здоровью человека;
- блокирование на неосознаваемом уровне свободы волеизъявления человека, искусственное привитие ему синдрома зависимости;
- утрата способности к политической, культурной, нравственной самоидентификации человека;
- манипуляция общественным сознанием, а также нарушении иных жизненно важных интересов личности, общества и государства.

Источниками угроз информационно-психологической безопасности являются: 1) физические лица, обладающие природными способностями воздействия на психику людей; 2) разработка программных и технических средств; 3) религиозные и иные группы; 4) антропогенные зоны; 5) геопатогенные зоны.

Объекты угроз

Отдельные граждане, представляющие различные возрастные, социокультурные и национальные группы и слои общества.

Отдельные социальные группы и слои как компоненты социальной структуры общества (в том числе профессиональные, национально-этнические и др.).

Отдельные организации, группы и лица, конкретные представители органов государственной власти и управления, Вооруженных сил, органов правопорядка и безопасности, производственных, финансовых и других структур, осуществляющие деятельность, которая имеет или может иметь важные социальные последствия.

Общественные и политические организации, общественно-политические движения и партии.

Население страны в целом как социально-историческая общность людей, обладающая специфическими особенностями общественной психологии.

Способы психологической защиты

Для обеспечения информационно-психологической безопасности личности можно рекомендовать различные способы психологической защиты. Они позволяют предотвратить или нейтрализовать негативное воздействие информации в различных ситуациях, контакт-коммуникационных и межличностных.

Способ защиты 1-й: «Уход» - увеличение дистанции, прерывание контакта, выход за пределы досягаемости информационного воздействия. Действия в различных информационных ситуациях могут быть такими:

- отключение определенных каналов СМИ (раздражающего канала телевидения, выход из Интернета и пр.), отказ от просмотра (прослушивания) конкретных теле-радиопрограмм;
- отказ от чтения некоторых газет, статей, рубрик и пр.;
- уход под различными предлогами с массовых зрелищных мероприятий: театра, концертного зала, кинотеатра и пр., митингов, собраний и др.;

- смена неприятной темы беседы, стремление не обострять межличностные отношения во время беседы.

В некоторых случаях защита может выразиться в более резких формах – **«изгнании»** или **«игнорировании»**.

При использовании способа **«изгнание»** средство или источник негативного информационного воздействия изгоняется (или вытесняется) из информационной среды (отказ от пользования телевизором или компьютером, отказ посещать театральные постановки или концерты и пр.).

«Игнорирование» предполагает не восприятие информации, которая затрудняет или препятствует определенной деятельности человека, может спровоцировать конфликт, вызвать негативные эмоции.

Способ защиты 2-й: «Блокировка» - контроль информационного воздействия, выставление психологических барьеров, ограждение психики от внешнего негативного информационного воздействия.

Действия, выполняемые при «блокировке»:

- критическое восприятие информации;
- эмоциональное отчуждение (восприятие негативной информации «без эмоций»);
- увеличение межличностного пространства – «зоны общения» во время беседы;
- использование «психологических барьеров» (принижение источника информации, внутреннее осмеяние, развенчание авторитета, несерьезное восприятие информации, недоверие, настороженность, невнимательность, отвлечение и переключение внимания на другие объекты, не связанные с содержанием информационного воздействия и пр.).

Способ защиты 3-й: «Управление» - контроль процесса информационного воздействия, влияние на его характеристики и источник. Выполняемые действия:

- использование обратной связи (участие в опросах рейтинга популярности определенных каналов или программ телевидения, популярности периодических изданий и пр.);
- выражение в зрелищных мероприятиях своего отношения к происходящему (неодобрения, недовольства выступающими);
- использование при беседе принципа «своих не обижают», для чего продемонстрировать желание стать другом, членом одной общности; ослабить или дестабилизировать активность собеседника неожиданным отвлечением (например, сделать комплимент, высказать сочувствие) и др.

Способ защиты 4-й: «Затаивание» - контроль своей реакции на внешнее информационное воздействие. Выполняемые действия:

- отсрочка своих реакций, поспешных выводов и оценок, задержка или отказ от действий и поступков, вызываемых информационным воздействием (например, при нахождении в толпе, чтобы не поддаться «эффекту толпы»)
- маскировка, сокрытие чувств, проявлений эмоций и др.

Умение человека в зависимости от ситуации воспользоваться тем или иным способом психологической защиты от негативного воздействия информации способствует формированию его информационной культуры, которая, в конечном счете, и обеспечит информационно-психологическую безопасность личности.

Заключение

В теории и практике информационной безопасности можно выделить два направления: защита информации и информационно-психологическая безопасность. Информационно-психологическая безопасность создает условия для обеспечения психического здоровья отдельной личности и населения страны в целом, надежного функционирования государственных и общественных институтов, а также формирования индивидуального, группового и массового сознания, нацеленного на прогрессивное развитие общества. Информационная безопасность – залог устойчивого развития экономики и общества.

Для безопасной работы в сети Интернет мной была разработана Памятка Интернет-пользователя, которая сможет помочь обеспечить свою безопасность в информационном пространстве (см. Приложение).

Приложение

Список используемых источников:

1. Доктрина информационной безопасности Российской Федерации. М., 2002.
2. Аносов В.Д., Стрельцов А.А., О Доктрине информационной безопасности Российской Федерации // Информационное общество. 1997. № 2–3. С. 3–9.
3. Аносов В.Д., Лепский В. Е., Стрельцов А. А., Проблемы обеспечения информационно-психологической безопасности // Информационное общество. 1997. № 4–6.
4. Арсентьев М.В., к вопросу о понятии «информационная безопасность»// Информационное общество. 1997. № 4–6.
5. Геополитика и национальная безопасность: Словарь основных понятий и определений / М. И. Абдрахманов и др. М., 1998.

6. Емельянов Г.В., Стрельцов А.А., Информационная безопасность России: Учеб. пособие/ Под общ. ред. А. А. Прохожева. М., 1999. Ч. 1: Основные понятия и определения.
7. Емельянов Г.В., Стрельцов А.А., Проблемы обеспечения безопасности информационного общества // Информационное общество. 1999. № 2.

СВОБОДА СЛОВА И МЕДИА-ИНФОРМАЦИИ В ИНТЕРНЕТЕ

Хасанова Арина Дамировна
ОГБПОУ «Колледж индустрии питания, торговли и сферы услуг»
Руководитель: Лукьянова Наталья Петровна

Введение

Каждую секунду человек запускает свой телефон или компьютер и выходит в глобальную сеть, но никто не задумывается о том, как информация внутри этой сети влияет на его психическое состояние.

В связи с широкой информатизацией информационная сфера стала важной частью общественной жизни. Интернет находится повсюду: в наших домах, в наших карманах, в наших ушах. Информация окружает нас беспрерывно.

Цель проекта: изучив основные и знакомые понятия, рассказать о возможности защиты психологического состояния человека от переизбытка информации. Ведь сеть – это не только плюсы.

М. Бакунин писал: “Свобода одного человека заканчивается там, где начинается свобода другого”, но в Интернете эти рамки полностью стираются. В сети каждый человек волен высказывать своё мнение и критику в сторону другого человека, и такая критика не всегда адекватна. Социальные сети в этом плане сильно усложнили жизнь и взаимодействие с людьми и добавили кучу возможностей нарушения чужих границ, только мы можем разобраться в этом и миниминизировать вред, который мы наносим другим людям своими сообщениями или комментариями. Но мы не задумываемся об этом. Все мы знаем такие слова как: Интернет или медиа, но, я думаю, никто не задумывается о том, как в совокупности эти слова влияют на человека и его психическое состояние. И сегодня я постараюсь рассказать вам об этом и о том, как защитить себя в Интернет-пространстве.

Основные понятия

Интернет — всемирная система объединённых компьютерных сетей для хранения и передачи информации. Часто упоминается как Всемирная сеть и Глобальная сеть, а также просто Сеть;

Свобода — как возможность индивида самому определять свои жизненные цели и нести личную ответственность за результаты своей деятельности;

Свобода слова — право человека свободно выражать свои мысли. В настоящее время включает свободу выражения, как в устной, так и в письменной форме (свобода печати и средств массовой информации); право выражать мнения и идеи беспрепятственно и, главное, не боясь быть наказанным за это;

Медиа — это собирательное название средств массовой информации. Латинское слово **Medium** означает «посредник, середина», так что медиа это те, кто стоит посередине между читателями и источниками новостей. От этого же слова произошло понятие «социальных медиа» — популярных сайтов, которые заменяют собой СМИ благодаря обмену информацией между пользователями;

Информация — это, во-первых, специфический атрибут объективного мира (в том числе жизнедеятельности личности, общества, государства), создающий условия, необходимые для обеспечения устойчивости и развития систем различной природы; во-вторых, универсальную субстанцию, пронизывающую все сферы человеческой деятельности, служащую проводником сведений и знаний, инструментом общения, взаимопонимания и сотрудничества, утверждения стереотипов мышления и поведения; в-третьих, сведения (данные) о лицах, предметах, фактах, событиях, явлениях и процессах, которые могут быть переданы от одного объекта или субъекта к другом в виде сообщений, независимо от формы их представления (социальной, машинной, биологической и т.д.); в-четвертых, передаваемые от организма к организму признаки и их смысловое разнообразие.

Информационно-психологическая безопасность (в отношении личности) — состояние защищенности отдельных лиц и (или) групп лиц от негативных информационно-психологических воздействий и связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере;

Информационное пространство — совокупность банков и баз данных, технологий их сопровождения и использования, информационных телекоммуникационных систем, функционирующих на основе общих принципов и обеспечивающих:

- информационное взаимодействие организаций и граждан;
- удовлетворение их информационных потребностей.

Основными компонентами информационного пространства являются: информационные ресурсы, средства информационного взаимодействия и информационная инфраструктура;

Информационная сфера – сфера деятельности, связанная с созданием, сбором, преобразованием, хранением, распределением, и использованием информации.

Что такое свобода слова в интернете?

С правовым регулированием права на свободу слова в Интернете связано огромное количество проблем, так как во многих случаях существует вполне реальная угроза усиления давления на общественное мнение, введения цензуры, а также фальсификации фактов со стороны государства, нарушения прав человека на доступ к достоверной информации.

Я провела статистику и выявила, что свобода слова в Интернет сети разная во всех государствах, например, в КНДР доступ к сети Интернет имеют лишь высокопоставленные партийные деятели, а также пропагандисты идеологии Чучхе за рубежом. Всё остальное население имеет доступ лишь к внутренней сети “Кванмен”, являющейся локальным аналогом сети Интернет, но распространяющей исключительно пропаганду идей Чучхе среди граждан рес-

публики. Но самое жесткое регулирование сети Интернет получает Узбекистан, где каждый веб-сайт должен быть зарегистрирован в органах власти наряду с другими средствами массовой информации, что обеспечивает тотальный контроль за информацией, предоставляемая этими информационными ресурсами.

Таким образом, свобода слова в подобных государствах полностью отрицается, люди лишены возможности получать достоверную информацию, следовательно, не способны защищать и другие свои права.

Государства следят за информацией в Интернете, но совсем не следят за тем, что происходит между людьми в Интернет-сети.

Как реагировать на критику в Интернете?

В интернете может подвергнуться критике всё. Как вы пишите, как вы одеваетесь, что едите, как ставите пробелы между словами и прочее. То, что совсем не касается других людей, может стать объектом их обсуждения. И аргумент: “если ты выкладываешь что-то в сеть – будь готов и к критике!” – неверный, но рамки личного пространства в интернете давно стёрлись, поэтому нужно знать, как вести себя, если вы подверглись критике или осуждению:

1. Во-первых, нужно помнить, что любая критика, если она не является желанной, не стоит вашего внимания.

2. Во-вторых, критика – это хайп. Вы привлекли внимание своим внешним видом? Словами или же образом жизни? За вами бежит толпа хейтеров, которая не теряет возможности написать о вас гадости на каждом углу? Помните, что, в первую очередь, они привлекают заинтересованных в вас людей.
3. И, в-третьих, будет намного лучше, если вы ответите спустя какое-то время, за которое с «остывшей» головой, сможете обдумать наиболее удачный вариант ответа;

Берегите себя и свои нервы.

Медиа-контент в сети

Для полноты картины приведу немного статистики, выуженной все в том же бездонном Интернете:

- За последние три десятилетия было произведено больше информации, чем за предшествующие 5000 лет.
- Объем печатной продукции удваивается каждые 4-5 лет.
- Каждый день в мире издается более 4000 книг.
- Прежде чем современный ребенок достигнет совершеннолетия, он успеет посмотреть более 140 тыс. рекламных роликов.

Информация в СМИ и сети Интернет идёт нескончаемым потоком. Она не всегда является достоверной и полезной, что несёт вред человеческому мозгу. Ваша голова не помойка и она достойна лишь качественного контента. К потреблению информации нужно подходить осознанно, также, как и к продуктам, которые вы отбирается для вашего употребления. Информация, на которую опирается человек, строит его действительность, определяет его мировосприятие. Поэтому следует быть осознанным в восприятие поступающей информации.

На данный момент посредством осмысления всей картины современного мира были выявлены проблемы информационного характера:

- Переизбыток информации и невозможность ее осмысления в полной мере.

– Так называемый **«информационный шум»**, то есть переизбыток не всей информации в целом, а именно той, которая является не нужным человеку, например, в интернете это всевозможная вирусная реклама, спам на электронной почте и т.д.
– Манипуляция массами людей посредством СМИ.
– Постепенная замена критического мышления шаблонным.

Хотелось бы уделить особое внимание о том, как же обезопасить своего ребёнка?

Через мониторы компьютеров угроз на детей обрушивается отнюдь не меньше. Одна из опасностей - ***кибербулинг***: запугивание, психологический и физический террор - до чувства страха и подчинения. В Интернете насилие такого рода не редкость, как и различный агрессивный и нежелательный контент, мошенничество, сексуальное домогательство. Конечно, Интернет не только источник угроз, он открывает большие возможности для общения и саморазвития. Чтобы Интернет приносил пользу, а не вред, родителям необходимо **научить** детей правилам безопасного пользования Сетью так же, как они учат их не переходить дорогу на красный свет светофора.

Заключение

Подводя итог, хочется сказать, нет ничего плохого в том, что мы не запоминаем всю информацию. Это и есть наш предохранительный клапан, защищающий мозг от обработки хаотичных внешних раздражителей. Но это защитное устройство не может полностью оградить нас от огромного количества данных, поступающих из внешнего мира. Когда информации слишком много мозг «зависает», как компьютер. Лучше всего усваивается та информация, которая обладает для нас смыслом. Мы запоминаем то, что вызывает у нас ассоциации, эмоции, мысли. Отрывочные бессвязные сведения не представляют для человека ценности, но могут вызывать переутомление нервной системы, порождая ощущение хаоса, беспомощность и вызывая раздражительность. В этом и есть вред компьютера на психическое состояние человека.

Так как же не потонуть в информационном потоке? Наверное, каждый думающий и заботящийся о своем душевном здоровье человек находит для себя свой способ. Для некоторых он заключается в том, чтобы в меру сил фильтровать этот огромный поток, не быть всеядным и бездумным потребителем, стараться не жить на автомате и прежде чем делать тот или иной выбор задавать себе вопрос: нужно ли мне это и хочу ли я этого (мое ли это желание)?

Список используемых источников:

1. https://cyberleninka.ru/article/v/informatsionno-psihologicheskaya-bezopasnost-osnovnye-polozheniya
2. http://cdo-revda.edusite.ru/p929aa1.html
3. http://constructorus.ru/zdorovie/informacionnaya-peregruzka.html
4. file:///C:/Users/student/Downloads/s025-038.pdf
5. http://gutta-honey.livejournal.com/298998.html
6. http://www.vitamarg.com/konsultacii/life/2275-pereizb
7. http://refleader.ru/otrbewpolujg.html
8. https://dic.academic.ru/
9. https://cyberleninka.ru/article/n/svoboda-slova-v-seti-internet

НЕЙРОЛИНГВИСТИЧЕСКОЕ ПРОГРАММИРОВАНИЕ

Максимов Сергей Александрович
ОГБПОУ «Томский индустриальный техникум»
Руководитель: Асадулина Галия Спартаковна

Предмет исследования

Влияние нейролингвистического программирования на свойства информации.

Актуальность исследования

Нейролингвистическое программирование - направление современной практической психологии, очень популярное как на Западе, так и в России. Однако не все представляют себе, что это такое, и почему данное направление психологии приобретает все большую популярность. В данной работе будет рассмотрено влияние НЛП на психологию и восприятие жизни и исторических событий людьми.

Методы исследования

1. Социологический опрос.
2. Изучение интернет-ресурсов по теме.
3. Личные наблюдения

Нейролингвистическое программирование (НЛП) - направление современной практической психологии. НЛП родилось относительно недавно.

Возникнув в 1975 г. как методология эффективного общения в чистом виде, нейролингвистическое программирование быстро доказало свою практическую ценность; с 1984 г. оно активно используется в предвыборных кампаниях самого высокого уровня, и это — признание в мире рекламы.

Впервые в России заговорили об НЛП в конце 80-х, когда стали появляться первые подпольные переводы книг, и в рамках культурного обмена проводились короткие тематические семинары.

Сегодня нейролингвистическое программирование - наиболее распространенный инструмент манипулирования массовым сознанием.

Реклама, по сути, является средством манипулирования, а результат ее действия — формирование общественного мнения.

Используя НЛП-подход, реклама должна смоделировать стратегию покупки и внедрить ее в мышление потребителя (разве это не манипулирование сознанием?).

Чем же хороша приведенная стратегия, которую демонстрирует реклама компании «Жиллет»? Даже если вы предпочитаете бритвы другого производителя, без сомнения, вы когда-либо пользовались или хотя бы знаете о продукции «Жиллет». Реклама «Жиллет» рассчитана на то, чтобы не слишком дорогие и не слишком крупные вещи люди покупали импульсивно (для себя или в подарок кому-то). Мужчинам часто дарят бритву женщины, которые сами этим предметом не пользуются, поэтому даже если первое лезвие бреет отвратительно, а второе не бреет вообще, будет куплен тот предмет, который лучше рекламируется. [2]

Другое направление НЛП – это влияние на осознание людьми истории своей страны. Рассмотрим Россию и некоторые окутавшие ее мифы. 400 лет информационных войн. Знаем ли мы свою страну, и почему русскому просвещенному человеку легче поверить иностранному агенту? Почему информационная война против России началась именно во времена Ивана Грозного?

Информационные источники с запада порой попадали в цель и в самой России. Жители начинали верить, что именно так беспросветно и выглядят их прошлое и настоящее. И мало кого волновало, что не сходится число жертв новгородской резни – 300 тысяч, как передают некоторые авторы. А во всем Новгороде в то время жило от силы 10 тысяч человек.

Беспричинный террор - это самый главный аргумент против Ивана Грозного. Мол, исключительно ради забавы резал грозный царь ни в чем не повинных бояр. Хотя периодическое возникновение широко разветвленных заговоров в боярской среде не отрицает ни один уважающий себя историк, хотя бы потому, что заговоры - обычное дело при любом царском дворе. А многих

якобы казненных бояр наподобие братьев Воротынских, умертвили исключительно историки, а не Грозный. Исследователи-историки немало веселились, находя документы о жизни многих бояр, как ни в чем не бывало продолжавшейся и после того, как им будто бы отрубили голову или посадили на кол. При Иване Русь поднялась с колен и расправила плечи от Балтики до Сибири. При вступлении на престол Иоанн унаследовал 2,8 млн. кв. км, а в результате его правления территория государства увеличилась почти вдвое - до 5,4 млн. кв. км - чуть больше, чем вся остальная Европа. За то же время население выросло на 30-50% и составило 10-12 млн. человек. При Иване окончательно были уничтожены остатки феодальной раздробленности, а без этого неизвестно, пережила бы Россия смутное время или нет. По велению Ивана Грозного было возведено свыше 40 каменных церквей, украшенных золотыми куполами. Царь основал 60 монастырей, подарив им купола и украшения, а также пожертвовав им денежные вклады. Иоанн IV, под именем Парфения Юродивого, написал Канон и молитву архангелу Михаилу, назвав его именно Грозным Ангелом. Канон подчеркивает священный страх, исходящий от архангела, здесь он описан, как "грозный и смертоносный". Царь Иоанн писал еще и стихиры, о которых очень высоко отзываются знатоки нашей древней письменности.

Отечественная история загромождена мифами западного происхождения, созданными специально, чтобы принизить русскую историю. [3]

Другой пример – это царствование Павла I, объявленного чуть ли не сумасшедшим. На самом деле Павел правил гуманней, чем его мать Екатерина Вторая, особенно по отношению к простому люду, солдатам. А. И. Тургенев, оценивая деятельность императора, писал: «Народ был восхищен, был обрадован, приказания Его чтил благодеянием, с неба посланным… Дозволяю себе смело и безбоязненно сказать, что в первый год царствования Павла народ блаженствовал, находил суд и расправу без лихоимства, никто не осмеливался

грабить, угнетать его…» Однако его прозвали «злодеем» за то, что он увольнял нерадивых сановников, начальников и даже выслал из столицы (!) в другие города европейской части России (вот это злодей!) несколько сотен человек.

Враги Павла ещё при его жизни, а после смерти особенно (стараясь прикрыть своё участие в заговоре и убийстве законного правителя России), распускали слухи, что он сошёл с ума. Каждый поступок императора дополняли такими подробностями, ретушировали, чтобы представить его больным. В результате дурная слава быстро разошлась по дворянским салонам России. А в Европе её с удовольствием подхватили. На Западе всегда с особенной радостью воспринимали любые дурные известия из России, перевирали факты (это не изменилось и в настоящее время). Так сложилась ситуация, что даже сейчас для большинства обывателей император Павел — это «дурачок на троне», царственный сумасброд или «сумрачный и подозрительный тиран», душивший любые проявления свободы. [4]

Согласно статье 55 Конституции РФ право на доступ граждан к информации может быть ограничено в только в отношении информации, отнесённой к государственной или коммерческой тайне. А одним из важнейших показателей информации является адекватность, то есть соответствие информации реальному, объективному состоянию дела (объекта, явления).

К сожалению многие исторические события в нашей стране описывались иностранными историками, служившими при дворе, которым выгодно было представлять Россию нищей, убогой и безграмотной. А навязывание нам неверных исторических фактов не что иное, как НЛП. Из всего выше сказанного следует, что существует неразрывная связь между НЛП и информационной безопасностью, а именно в той ее части, что касается целостности и адекватности.

Мною был проведен опрос среди студентов и работников техникума:

Знаете ли Вы что такое НЛП?	да	нет

Покупаете ли товары, ориентируясь на рекламу?	да	нет	иногда
Верите ли Вы средствам массовой информации?	да		нет
Иван IV	тиран	великий политик Отечества	не знаю, кто это
Павел I	самодур, сошедший с ума	достойный приемник Екатерины II	не знаю, кто это

Опрос относительно первых 3-х вопросов показал: 70% студентов 2 курса не знают, что такое НЛП; 50% всегда покупают товары, ориентируясь на рекламу, 30% лишь иногда поддаются рекламе, а 20% на рекламу не реагируют; 70% не верят средствам массовой информации.

Опрос относительно мнения о двух правителях нашей страны Иване IV и Павле I показал, что из категории опрошенных моложе 18 лет 90% назвали Ивана Грозного тираном, 10% вообще не знают, кто это. В то время как в категории старше 25 лет 60% ответили «тиран», а 40% выбрали ответ «великий политик отечества». На вопрос о Павле I из категории опрошенных моложе 18 лет 80% ответили «самодур, сошедший с ума», из категории старше 25 лет практически столько же - 70%.

Заключение

НЛП – это направление психологии, доведенное до точности технологии. Надо, чтобы от НЛП было больше пользы, чем вреда. Лечению больных людей – ДА, обману и переписыванию истории – НЕТ. Мы, молодежь, хотим гордиться историей нашей страны и политикой, проводимой президентом в настоящее время. Поэтому, чтобы не подвергнуться влиянию НЛП, следует получать информацию из различных источников, ориентируясь также на своей жизненный опыт и опыт своих старших родственников и знакомых. Необходимо владеть навыками информационной культуры и в принципе быть

грамотным и всесторонне развитым человеком. Влиять на сознание образованного человека труднее.

Список используемых источников:

1. Герасимов А. НЛП в рамках психотерапии http://www.nlpcenter.ru/literat/articles/ger_nlp.htm
2. Князев С. Нейролингвистическое программирование, технологии в рекламе. http://nlpr.ru/node/182
3. https://russia.tv/brand/show/brand_id/49303/
4. Самсонов А. Миф о «сумасшедшем императоре» Павле I https://topwar.ru/59322-mif-o-sumasshedshem-imperatore-pavle-i.html

СПОСОБЫ ПСИХОЛОГИЧЕСКОЙ ЗАЩИТЫ

Данилова Карина Сергеевна
МОУ «Школа № 45 г. Донецка»
ДНР
Руководитель: Нетребская Татьяна Борисовна

Аннотация: в работе раскрыта психология защитного поведения, уровни и механизмы функционирования психологической защиты личности, стратегии защитного поведения.

Тема психологической безопасности все чаще поднимается в современном мире и рассматривается с самых разных сторон: от мирового терроризма, в том числе и психологического, когда субъектом выступает все мировое сообщество, до экологичности воздействия на какую-либо характеристику личности при психологическом консультировании, где субъектом является индивид. Это отражается в культуре: вопрос зомбирования, управления человеком поднимается в литературе, кино, в сводках новостей, тема воздействия на человека и способы защиты от этого затрагиваются в связи с выборными компаниями, рекламой услуг и продуктов.

Психологическая защита согласовывает сознательное и бессознательное в человеке. Она ослабляет внутренний конфликт между индивидуальным и коллективным бессознательным. Смягчению внутреннего конфликта также способствуют элементы сознания: рассудительность и способность логически мыслить, внимание, память, оптимизм и жажда жизни. Ясность мышления, способность посмотреть на себя со стороны (иногда с юмором) — основные критерии высокого уровня психологической защищенности человека.

Актуальность темы данной работы состоит в том, что понятие психологической защиты является одним из основополагающих в современной теории личности. Оно обладает большой объяснительной силой при изучении патогенеза психических и психосоматических заболеваний. Тем не менее, широких и систематических исследований, направленных на изучение соотношения

различных механизмов психологических защит в норме и патологии, проведено немного.

Любой человек имеет определенную систему психологической защиты, которая обеспечивает иммунитет от разрушающих влияний на ее личность. Самая сила защиты зависит от врожденных и приобретенных за жизнь психологических особенностей человека и его знаний. Таким образом, даже простая осведомленность о методиках изменения личности может дать возможность довольно успешно противостоять психологическим влияниям, откуда бы они не поступали. Сломать психологическую защиту личности, действуя простым убеждением, в большинстве случаев не удается. Чтобы проникнуть во внутренний мир человека и руководить им, используют специальные приемы психологического влияния.

Ведь человек, который умеет управлять собой и своими поступками в отдельной ситуации скорее сможет управлять ходом событий собственной жизни вообще. И наоборот, человек, не имеющий навыков самостоятельной переработки информационных потоков, имеет потенциальную опасность попасть под негативное психологическое влияние другого человека или группы людей. Еще страшнее, когда подобное психологическое влияние есть деструктивным, направленным на подчинение воли человека чьим-то интересам: политическим, коммерческим, религиозным и т.д.

Рассмотрим некоторые наиболее распространенные определения психологической защиты. Она определяется как:

- психическая деятельность, направленная на спонтанное изживание последствий психической травмы (В. Ф. Бассин, В. Е. Рожнов, 1975);
- частные случаи отношения личности больного к травматической ситуации или поразившей его болезни (В.М. Банщиков, 1974);
- способы переработки информации в мозге, блокирующие угрожающую информацию (И.В. Тонконогий, 1978);

- механизм адаптивной перестройки восприятия и оценки, выступающей в случаях, когда личность не может адекватно оценить чувство беспокойства, вызванное внутренним или внешним конфликтом, и не может справиться со стрессом (В.А. Ташлыков, 1984);
- механизмы, поддерживающие целостность сознания (В.С. Ротенберг, 1984);
- механизм компенсации психической недостаточности (В.М. Воловик, В.Д. Вид, 1975);
- пассивно-оборонительные формы реагирования в патогенной жизненной ситуации (Р.А. Зачепицкий, 1980);
- динамика системы установок личности в случае конфликта установок (Ф.В. Бассин, 1976);
- способы репрезентации искаженного смысла (В.Н. Цапкин, 1985).

В широком смысле термин "психологическая защита" употребляется для обозначения любого поведения, устраняющего психологический дискомфорт. Это целая система привычных реакций человека, которая помогает устранить, или, если это невозможно, свести к минимуму негативные, травмирующие личность переживания.

Одним из наиболее применяемых методов исследования механизмов психологических защит в настоящее время является методика "Индекс жизненного стиля" - личностный опросник, предназначенный для диагностики механизмов психологической защиты "Я". Предложен Р. Плутчиком, Г. Келлерманом и Г. Конте в 1979г.

Методика представляет собой опросник, который состоит из 97 утверждений, предполагающих две градации ответа: "верно" или "не верно". Оценка степени использования механизмов психологической защиты проводится по следующим шкалам, каждая из которых включает от 10 до 14 вопросов:

1. Отрицание - механизм, посредством которого отрицаются некоторый причиняющий страдания опыт, некоторые импульсы или стороны себя. Информация, противоречащая установкам, не принимается.

Особенности защитного поведения: эгоцентризм, внушаемость и самовнушаемость, общительность, стремление быть в центре внимания, оптимизм, непринужденность, дружелюбие, умение внушить доверие, уверенная манера держаться, жажда признания, самонадеянность, жалость к себе, обходительность, готовность услужить, аффективная манера поведения, пафос, легкая переносимость критики и отсутствие самокритичности.

2. Вытеснение - механизм, посредством которого неприятные эмоции блокируются посредством забывания реального стимула и всех объектов и обстоятельств, связанных с ним.

Особенности защитного поведения: бессознательное избегание ситуаций, которые могут стать проблемными и вызвать страх, неспособность отстоять свою позицию в споре, соглашательство, покорность, робость, забывчивость, боязнь новых знакомств, выраженные тенденции к избеганию и подчинению подвергаются рационализации, а тревожность - гиперкомпенсации в виде неестественно спокойного, медлительного поведения, нарочитой невозмутимости и т.п.

3. Регрессия - избегание субъектом тревоги путем возвращения к онтогенетически более незрелым формам поведения и удовлетворения потребностей.

Особенности защитного поведения: слабохарактерность, податливость чужому влиянию, неумение доводить дело до конца, легкая смена настроения, плаксивость, в эмоционально напряженной ситуации повышенная сонливость и неумеренный аппетит, манипулирование мелкими предметами, непроизвольные движения, специфическая "детская" мимика и речь, склонность к мистике и суевериям, обостренная ностальгия, непереносимость одиночества, потребность в стимуляции, контроле, подбадривании, утешении, поиск новых впечатлений, умение легко устанавливать поверхностные контакты.

4. Компенсация - попытка исправления или замены объекта, вызывающего чувство неполноценности, нехватки, утраты.

Особенности защитного поведения: поведение, обусловленное установкой на серьезную и методическую работу над собой, нахождение и исправление своих недостатков, преодоление трудностей, достижение высоких результатов в деятельности; серьезные занятия спортом, коллекционирование, стремление к оригинальности, склонность к воспоминаниям, литературное и другое творчество.

5. Проекция - механизм приписывания окружающим различных негативных качеств, мыслей, чувств, что формирует рациональную основу для непринятия других и принятия на этом фоне себя.

Особенности защитного поведения: гордость, самолюбие, эгоизм, злопамятность, мстительность, обидчивость, уязвимость, обостренное чувство несправедливости, заносчивость, честолюбие, подозрительность, ревнивость, враждебность, упрямство, несговорчивость, нетерпимость к возражениям, тенденция к уличению окружающих, поиск недостатков, замкнутость, требовательность к себе и к другим, стремление достичь высоких показателей в любом виде деятельности.

6. Замещение - механизм снятия напряжения путем переноса агрессии с более сильного или значимого субъекта на более слабый и доступный объект или на самого себя.

Особенности защитного поведения: требовательность к окружающим, скандальность, раздражительность, вспыльчивость, реакции протеста в ответ на критику, отсутствие чувства вины, просмотр соревнований или занятия боевыми видами спорта, предпочтение литературы и фильмов со сценами насилия, приверженность к деятельности, связанной с риском; тенденция к доминированию; склонность к занятиям физическим трудом.

7. Интеллектуализация - механизм подмены чувственной основы логическими резонами, предполагает произвольную схематизацию и истолкование событий с целью сформировать чувство субъективного контроля над ситуацией.

Особенности защитного поведения: старательность, ответственность, добросовестность, самоконтроль, склонность к анализу и самоанализу, основательность, осознанность обязательств, дисциплинированность, любовь к порядку, предусмотрительность, индивидуализм.

8. Формирование реакции - механизм трансформации импульсов и чувств, которые субъект по тем или иным причинам расценивает как неприемлемые, в их противоположности.

Особенности защитного поведения: неприятие всего "неприличного", например, связанного с человеческим телом, физиологией и отношениями полов; подчеркнутое стремление соответствовать общепринятым стандартам поведения, аккуратность, озабоченность "приличным" внешним видом, вежливость, любезность, респектабельность, бескорыстие, общительность, как правило, приподнятое настроение, воздержанность, морализаторство, желание быть примером для окружающих.

В качестве показателей психологической защиты фигурируют количественный показатель выраженности каждого МПЗ и показатели интенсивности системы психологической защиты в целом.

Неоспоримыми плюсами этой методики являются ее теоретическая обоснованность и валидность, целенаправленная многомерность и конструктивная простота. Время заполнения опросника составляет от 15 до 20 минут. Подсчет результатов осуществляется по бланку ответов, который является одновременно ключом.

Таким образом, под психологической защищенностью понимается относительно устойчивое положительное эмоциональное переживание и осознание индивидом возможности удовлетворения своих основных потребностей и обеспеченности собственных прав в любой, даже неблагоприятной ситуации, при возникновении обстоятельств, которые могут блокировать или затруднять их реализацию.

В качестве основного механизма обеспечения психологической защищенности выступает психологическая защита – специальная регулятивная система стабилизации личности, направленная на устранение или сведение до минимума чувства тревоги, связанного с осознанием конфликта. В соответствии с таким подходом в качестве основной ее функции рассматривается «ограждение» сферы сознания от негативных, травмирующих личность переживаний.

В широком смысле термин «психологическая защита» употребляется для обозначения любого поведения, устраняющего психологический дискомфорт, в результате которого могут сформироваться такие черты личности, как негативизм, появиться «ложные», замещающие деятельности, измениться система межличностных отношений.

Психологическая защита, понимаемая в узком смысле, ведет к специфическому изменению содержания сознания как результату функционирования ряда защитных механизмов: подавления, отрицания, проекции, идентификации, регрессии, изоляции, рационализации, конверсии и др.

В самом общем виде информационно-психологическую безопасность личности целесообразно рассматривать как состояние, которое позволяет полноценно развиваться, своевременно адаптироваться к меняющимся социальным условиям и организовывать свое поведение (жизнедеятельность), позволяющее удовлетворять основные потребности в обществе в социально приемлемых формах с учетом интересов и деятельности других людей и действующих социальных институтов.

Список используемых источников:

1. Бассин Ф.В., Бурлакова М.К., Волков В.Н. Проблема психологической защиты // Психологический журнал. – 1996. – Т.9. - № 3. – С.78-87.
2. Грановская Р.М. Элементы практической психологии // URL: https://psy.wikireading.ru/58870
3. Грановская Р.М. Защита личности. – М.: Знание, 1999. – 352 с.

4. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты // URL: http://bookap.info/psywar/grachev/gl20.shtm
5. Морозов А.В. Способы психологической защиты // URL: http://student.km.ru/ref_show_frame.asp?id=4C5647559E3649F690CE113C0E5AE533
6. Платонов Ю.П. Приемы психологической защиты // URL: http://www.elitarium.ru/2007/07/16/priemy_psikhologicheskojj_zashhity.html
7. Психоаналитические термины и понятия: Словарь / Под ред. Б.Э. Мура и Б.Д. Фаина; Пер. с англ. — М.: Класс, 2000. — 304 с.

ВЛИЯНИЕ ИНТЕРНЕТ-СРЕДЫ НА ЛИЧНОСТЬ И ЕЕ ЖИЗНЕДЕЯТЕЛЬНОСТЬ

Беляева Ирина Олеговна
МОУ «Школа № 45 г. Донецка»
ДНР
Руководитель: Беляева Любовь Ивановна

Всемирная паутина стала для современного человека пространством, где не только можно находить интересующую информацию, но и жить. Все больше популярен шоппинг, заказ еды, оформление путевок, поиск новых знакомств в интернете. Можно сказать, что среднестатистический пользователь уже живет в интернете около 8 часов в сутки. В связи с этим актуальной становится проблема влияния интернет-среды на личность, ее развитие, жизнедеятельность. В работе рассматривается положительное и отрицательное влияние интернет-пространства на личность. Объектом исследования стал непосредственно интернет. Субъектом - личность и ее безопасность.

Поскольку возрастная категория пользователей интернет-пространством в последние годы значительно расширилась, то и мы объединим их по возрастным категориям:

- Дошкольный возраст (от 5 до 7 лет)
- Школьник (от 8 до 17 лет)
- Студент (от 18 до 25)
- Взрослый (от 26 до 45)
- Зрелый (от 46 до 69).

Дошкольному возрасту легче всего освоиться в новой среде. Дети быстро перенимают модели поведения более опытных пользователей. Чаще смотрят любимые мультфильмы или видео-блогеров на видео-площадке YouTube, чем заводят аккаунты и дополняют их. На таких сайтах очень маленький процент гневных комментариев или критики в адрес самих пользователей. Риск получить психологическую травму минимален. Опасность может подстерегать в виде рекламы. Случайно нажав на рекламу или уведомление,

сам того не зная, ребенок может открыть доступ к личным данным для злоумышленников. Дошкольники используют интернет как источник дополнительных позитивных впечатлений.

К подростковому возрасту формируется определенная зависимость от интернет-пространства. Установлено, что личность, использующая Интернет как продуктивный инструмент, характеризуется невысокой активностью в Сети. Если пользователь обладает высокой вовлеченностью виртуальной средой, неконструктивно использует интернет-среду, то развитие интернет-зависимости велико. Различные виртуальные способы самовыражения, повышенное желание коммуникации, за счет которой реализуется самопрезентация, выражаются в создании профилей в социальных сетях. Любимыми социальными сетями являются Instagram, Ask. Fm.

Данная возрастная группа не имеет достаточного опыта общения, не привыкла говорить о своих проблемах и внутренних переживаниях. Как следствие, принимая первую критику в сети, подросток начинает комплексовать. Чаще всего тинейджеру присылают анонимно оскорбления по поводу внешности, умственных способностей в независимости от пола. А в дальнейшем испуганный пользователь замыкается в себе, сильно занижается его самооценка и чувство собственной значимости. Важно объяснять, что критики в интернете не избежать, нужно лишь её правильно принимать. Часть анализировать, часть исправлять, но никогда не вступать в интернет-перепалку или доказывать обратное. Именно в этом возрастном диапазоне может произойти подмена реальности, виртуальный мир рассматриваться как реальный. Интернет в таком случае играет ведущую роль в жизнедеятельности личности.

Студенты чаще используют интернет для изучения новой информации, чем для развлечений. Чтобы глубже понять роль сети Интернет для студентов в настоящее время, можно изучить результаты опроса, проведенного среди студентов физико-математического факультета Марийского государственного университета в 2015 году. Целью опроса послужило изучение важности ресур-

сов сети Интернет в жизни каждого студента. Больше 50% студентов чувствуют себя в сети достаточно уверенно, справляясь с большинством задач. 70% опрошенных пользуются сетью Интернет с желанием занять свое свободное время. Треть студентов общаются в сети, при этом увеличивая знания по интересующим их предметам, оценивая Глобальную паутину как возможное средство реализации своих практических потребностей. Более 70% человек находят в Интернете много информации, полезной в будущей карьере. Но не стоит забывать и о внеучебной деятельности молодого поколения. Становясь старше, пользователи привыкают к критике, смело выражают свое мнение, не заботясь о последствиях. "Закаленный иммунитет" чаще всего разрушают взломы личных страниц. Вне зависимости от того, чем будут шантажировать – снимками, видео, перепиской интимного характера, такие действия всегда являются уголовно-наказуемыми. Ответственность за такую форму вымогательства предусмотрена. Но взломщик, в большинстве случаев даже не будет найден, останется за занавесом анонимности. Если даже парень или девушка попали в такую ситуацию, необходимо мыслить трезво. Иначе особо впечатлительные пользователи могут покончить с собой. Важно заранее взвесить каждое слово и фотографию в Интернете.

Категория взрослых использует интернет-пространство для работы, поиска новой информации. Редко пользуется услугами через сеть, предпочитая более старые и проверенные способы. Профили часто заводятся, временами дополняют их фотографиями. Риск взлома страниц не такой высокий, как у группы выше. Но мошенники могут воспользоваться и другими методами. Например, объявлениями о работе на дому. Данный вид мошенничества очень эффективно применяется в Интернете и хорошо работает на неопытных пользователях. На электронную почту жертвы приходит вполне убедительное письмо с предложением работать на дому за достойную плату. Работу предлагают самую разную - от выращивания клубники до переводов текстов и упаковки компакт-дисков. Обращение идёт от лица какой-либо компании.

Обычно работодатели сообщают, что для начала работы от вас требуется первоначальный взнос. Объясняется данное явление также разными способами - либо это залог, либо цена за обучение, либо что-то еще. Многие, даже не поинтересовавшись, что за компания собирается с ними работать, перечисляют положенную сумму мошенникам. После этого общение с мнимыми заказчиками заканчивается. Как следствие, обманутый пользователь остается один и без денег. Со временем развивается страх, недоверие ко всей интернет-среде. Важно популяризировать информацию о подобных видах мошенничества.

Группа зрелых пользователей пользуется ограниченным количеством сайтов, например, таким, как Skype, не воспринимают интернет-пространство как подростки. Для них компьютер служит проводником только до определенного ресурса. Поэтому психическое здоровье не нарушается.

Если обобщить в целом влияние интернет-среды на личность, то положительными моментами можно считать большое количество виртуальных друзей, отсутствие потери контактов с определенными людьми, готовность платить за особые возможности сети, улучшение самооценки. Факторов, отрицательно влияющих на личность, больше – это торможение развития, что выражается в отсутствии круга чтения, ухудшении коммуникативных навыков, увеличении ошибочных мнений, потере личностных контактов.

Таким образом, Интернет не только прочно вошел в жизнь человека, но и активно влияет на нее, изменяя качественно личностные характеристики пользователей.

Список используемых источников:

1. http://detionline.com/helpline/about
2. http://www.pewinternet.org/2014/10/22/part-1-experiencing-online-harassment/
3. https://goo.gl/YQxUNZ
4. http://pb.rcpsych.org/content/37/5/167
5. https://iom.anketolog.ru/2014/01/20/aktualnost-sociologocheskih-oprosov
6. https://cyberleninka.ru/article/n/vliyanie-internet-sredy-na-lichnost-i-ee-zhiznedeyatelnost

СРЕДСТВА ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА ОБЩЕСТВЕННОЕ СОЗНАНИЕ

Ревякин Антон Михайлович
МОУ «Школа №48 г. Донецка»
ДНР
Руководитель: Тюрикова Ольга Дмитриевна

ВВЕДЕНИЕ

Актуальность данной темы заключается в том, что в современном обществе средства массовой информации имеют большое значение. С их помощью оказывается воздействие на идеологию, культуру и традиции человека. Информационно-психологическая безопасность создаёт условия для обеспечения психического здоровья каждой отдельной личности и населения республики в целом, надёжного функционирования общественных и государственных институтов, а также формирования индивидуального, группового и массового сознания с целью прогрессивного развития общества.

Цель работы состоит в исследовании воздействия средств массовой информации на общественное сознание, а также изучении видов средств и степени их влияния на общество.

При выполнении работы применены следующие методы исследования:

- метод теоретического исследования через изучение научной литературы по теме исследования;
- метод социологического исследования – проведение опросов.

1. ВОЗДЕЙСТВИЯ НА ОБЩЕСТВЕННОЕ СОЗНАНИЕ

1.1. Каналы воздействия на общественное сознание

Проблема обеспечения информационно-психологической безопасности личности возникла совсем недавно. Под информационно-психологической безопасностью понимается состояние защищенности отдельных лиц и (или) групп лиц от негативных информационно-психологических воздействий и

связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере. За последние 10-15 лет заметно увеличилось количество исследований по данной проблеме и по вопросу влияния информационных технологий на сознание людей. Поэтому вопрос информационной безопасности человека остается открытым для изучения.

Следует заметить, что средства информационного воздействия на личность весьма разнообразны. Это семья, сфера образования, улица, книги, радио, кино, телевидение, массовая печать, аудиовизуальные средства. Эффективность воздействия информационных каналов на личность в современном обществе существенным образом повышается за счет активного развития и широкого применения новых информационных технологий.

Для исследования влияния различных каналов информационного воздействия на личность проведено анкетирование обучающихся общеобразовательной организации:

1. Какие каналы информационного воздействия на личность Вам известны?
2. Считаете ли Вы что поток рекламы, фильмы и передачи, пропагандирующие насилие, садизм, можно классифицировать как несанкционированный доступ к сознанию людей?
3. Верно ли, что «рекламная пауза» на телевидении воздействует на психику миллиона людей?
4. Являются ли источником информационного воздействия на общественное сознание компьютерные игры?
5. Какими нормативными документами Донецкой Народной Республики регламентируется информационная безопасность Вас как личности?
6. Часто ли Вы сталкиваетесь с рекламой в социальных сетях?
7. Считаете ли Вы что взлом Ваших аккаунтов, является информационным воздействием на Ваше сознание?

Проведя опрос среди учащихся 9, 10 и 11 классов было выяснено, что основными каналами воздействия являются интернет и телевидение, как показано на рисунках 1 и 2.

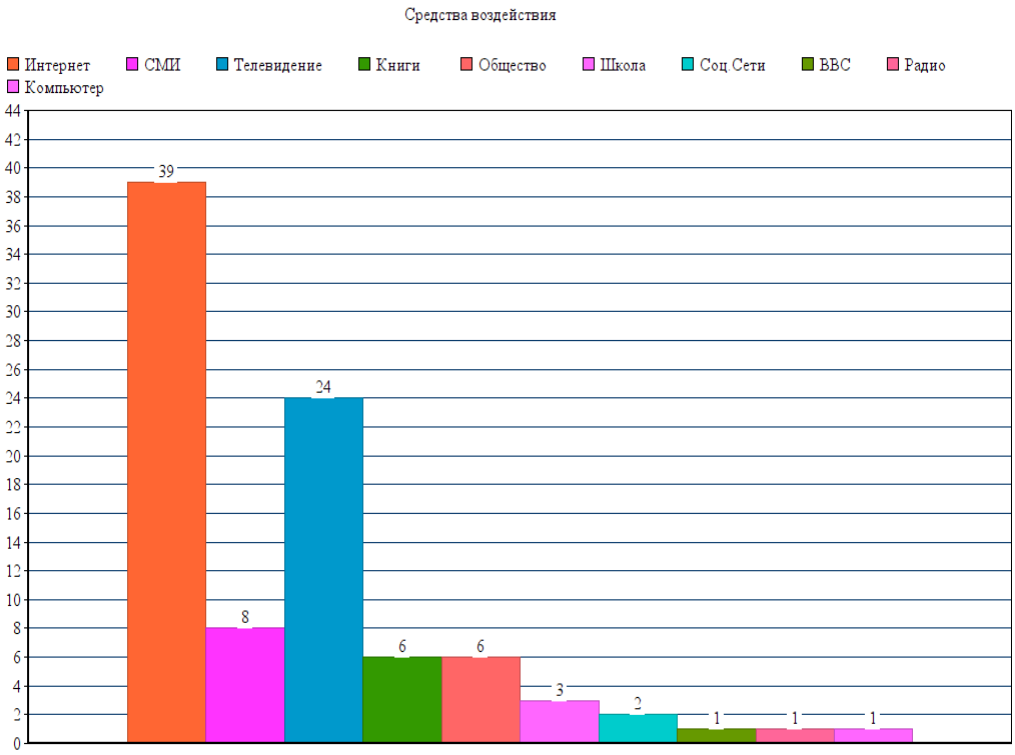


Рис.1. Средства информационного воздействия

Рис. 2. Каналы воздействия. Обобщенные данные

Также можно выделить компьютерные игры, как канал воздействия. Сюжеты игр повествуют о раздорах стран, глобальных конфликтах, ядерных войнах. Одни игры показывают одну страну агрессором, а другую героем-спасителем (при этом используются названия ныне существующих стран), другие продвигают идеи превосходства одной нации над другими.

Влияя на самый незащищённый сегмент общественной системы – молодёжь, компьютерные трактовки событий искажают факты политической

жизни. В умах людей формируются ложные идеи о политической действительности.

При социологическом исследовании на вопрос "Являются ли источником информационного воздействия на общественное сознание компьютерные игры?", из 41 опрошенного респондента 17 согласились с их частичным влиянием (рис. 3).

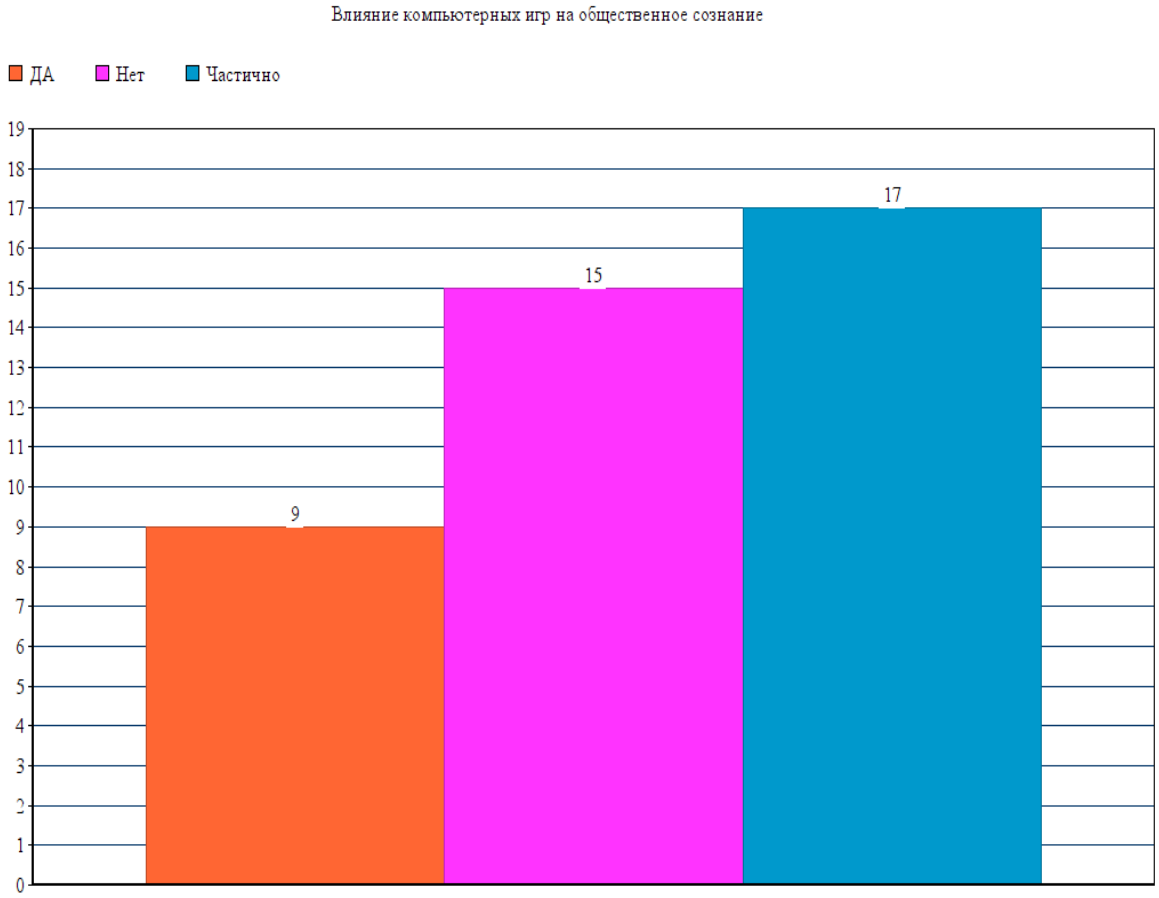


Рис. 3. Влияние компьютерных игр на сознание человека

Следовательно, разнообразные каналы воздействия можно использовать для оказания «нужного» информационного влияния на общественное сознание.

1.2. Технологии воздействия на общественное сознание

Теоретическую и методологическую основу изучения данного вопроса составляют научные исследования в области влияния на массовое сознание В.С. Комаровского, Д.М. Фетова. Авторами рассмотрены различные технологии воздействия на сознание личности. Наиболее часто используемые технологии:

1. Использование внушения. Источник вводит человека в суггестивное состояние. Индивид всё воспринимает на веру, не требуя доказательств.
2. Использование слухов, домыслов, толкований в неясной политической или социальной ситуации.
3. Эмоциональное воздействие на аудиторию с помощью крови, насилия, стрельбы, убийств и т.д.

В опросе из 42 человек, 20 согласились, что поток рекламы, фильмов и передач, пропагандирующих насилие можно называть несанкционированным доступом в сознание (рис.4).

4. Выбор наименьшего из двух зол.

В результате живописного рассказа о всей ужасности большего зла, меньшее представляется уже почти как добро.

5. Замалчивание одних фактов и выпячивание других.
6. Метод фрагментации.

Информационный поток разбивается на отдельные фрагменты не связанные друг с другом, в результате чего аудитории не удаётся сформировать правильной и полноценной картины мира.

7. Метод "Геббельса".

Откровенная ложь повторяется как можно чаще, чтобы публика в неё поверила.

8. Мистификация.

Выдаётся за факт событие, которого на самом деле не было.

Рис. 4. Несанкционированный доступ в сознание

Следует заметить, что в зависимости от возраста анкетируемого, восприятие технологий воздействия на сознание различно. Это подтверждается результатами анкетирования (рис.5, рис. 6, рис. 7).

Рис. 5. Результаты анкетирования учащихся 9 класса

Рис. 6. Результаты анкетирования учащихся 10 класса

Рис. 7. Результаты анкетирования учащихся 11 класса

Таким образом, в условиях информатизации общества информационные технологии становятся не только инструментом формирования потребностей, взглядов, ценностных установок, но и инструментом воздействия на мировоззрение человека в целом.

2. Роль СМИ в обществе

Роль СМИ в процессе формирования общественного сознания достигается оперативностью предоставления информации, доступностью, широким охватом аудитории, многоплановостью социальной ориентированностью.

Первоначальная задача СМИ заключается в освещении актуальных событий, информированностью населения, однако от типа и формы подачи информации, ее роль и влияние может меняться. Если негативные события в

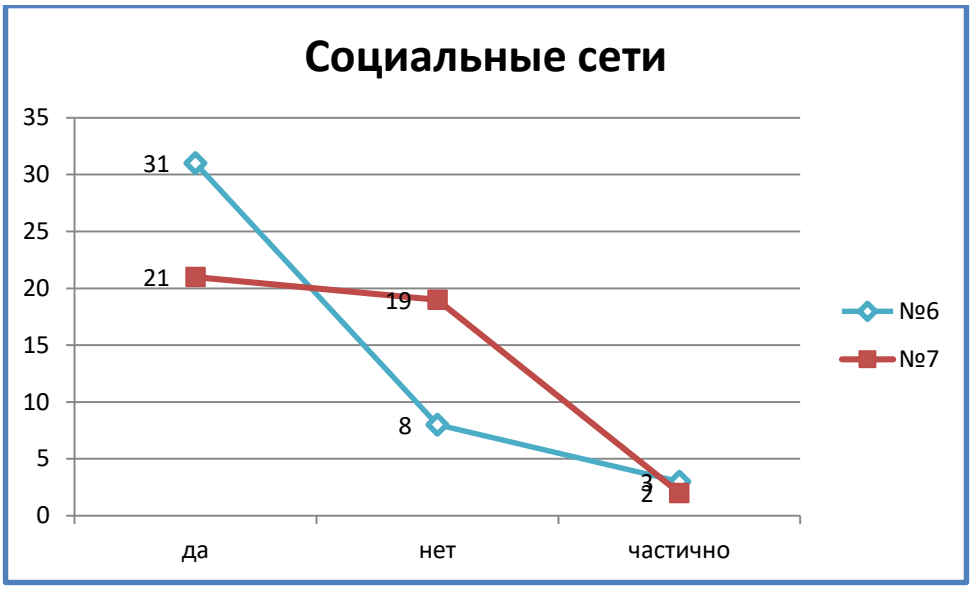
нашей стране подаются на фоне еще больших проблем в других государствах, традиционно собственные проблемы воспринимаются легче и не так губительно.

Развитие и распространение СМИ предоставляет практически неограниченный доступ к информационным ресурсам без учёта временных и пространственных рамок. С другой стороны – развитие СМИ привело к изменению назначения средств массовой информации: происходит изменение идеологических взглядов, наблюдается служение групповым интересам, процветает искажению фактов.

Роль СМИ в нашей жизни настолько велика, что без газет, журналов и телевидения человек вернется на несколько лет назад и будет оставаться в полном неведении о событиях в мире. Так как влияние СМИ на жизнь человека велико, то необходимо выбирать самые качественные средства массовой информации, на которые не влияют посторонние факторы, например, политика, экономическое влияние. Положительным фактором развития СМИ является то, что из всего массива информации всегда можно найти достойную и качественную, а из десятков газет – честную и справедливую, в которой все события освещаются точно, быстро и непредвзято.

Благодаря широким коммуникационным возможностям социальные сети также являются эффективным инструментом управления мировоззрением личности на современном этапе (рис.8). Общение, в том числе и виртуальное, играет важную роль для развития личности на каждом возрастном этапе. Виртуальная жизнь личности в социальных сетях приводит к тому, что становится сложнее определять эмоциональное состояние собеседника и поэтому труднее становится выбрать правильную линию поведения. А значит легче воздействовать на сознание. Немаловажную роль в воздействии на сознание играет и реклама, так легко распространяема в социальных сетях. Все чаще наблюдается взлом аккаунтов пользователей сети, что служит нарушением информационной безопасности. Информационная безопасность – это со-

стояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.



Акцентируя внимание на вышеизложенное, можно утверждать, что в условиях информационного общества человек подвержен одновременному влиянию печатных и электронных СМИ, радио и телевидения. Неправильное потребление информации может привести к непосредственному влиянию на формирование мировоззрения обучающегося. Поэтому информационная безопасность должна регламентироваться нормативно-правовыми документами, основной целью которых будет создание условий для снижения информационного воздействия на подрастающее поколение.

3. Нормативные документы Донецкой Народной Республики, регламентирующие информационную безопасность личности

При рассмотрении методов воздействия на массовое сознание необходимо рассматривать проблему эффективности ограничения применения нежелательных технологий и каналов воздействия на общественное сознание законодательными рамками. Именно нормативно-правовое поле должно определять «безопасность» и «корректность» подобных технологий, осуществлять контроль за информационно-психологическими процессами, проводить мониторинг неявных, скрытых воздействий на массовое сознание.

Для регулирования отношений в информационном пространстве в Донецкой Народной Республике принято ряд законов.

Закон Донецкой Народной Республики «Об информации и информационных технологиях», принятый Постановлением Народного Совета 07.08.2015 года, регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации. Кроме того, статья 9 «Ограничение доступа к информации» служит нормативной основой для обеспечения ограничения доступа к информации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Также Законом предусматривается установление ответственности за нарушение законодательства Донецкой Народной Республики об информации, информационных технологиях и о защите информации.

Закон Донецкой Народной Республики «О защите детей от информации, причиняющей вред их здоровью и развитию» регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции. В Законе сформулировано понятие «информационная безопасность детей» – состояние, при котором отсутствует риск, связанный с причинением информацией вреда здоровью и (или) физическому, психическому, духовному, нравственному развитию детей. Одна из статей названого Закона посвящена видам информации, причиняющей вред здоровью и (или) развитию детей.

Общественные отношения в сфере организации деятельности средств массовой информации регулирует Закон Донецкой Народной Республики «О средствах массовой информации». В Законе акцентируется внимание на запрете использования в радио-, теле-, видео-, кинопрограммах, документальных и художественных фильмах, а также в информационных компьютерных файлах и программах обработки информационных текстов, относящихся к

специальным средствам массовой информации, скрытых вставок и иных технических приемов, и способов распространения информации, воздействующих на подсознание людей или оказывающих вредное влияние на их здоровье.

Исходя из вышеизложенного можно сказать, что в Донецкой Народной Республике формируется нормативно-правовое поле, обеспечивающее защиту прав граждан от информационного воздействия на их мировоззрение.

ЗАКЛЮЧЕНИЕ

В данной работе было уделено внимание средствам информационного воздействия на общественное сознание.

Изучение воздействия на общественное сознание, роли СМИ в обществе, нормативных документов, которые регламентируют информационную безопасность личности, позволило обратить внимание на проблему информационного воздействия на личность различными средствами и технологиями. Акцентировано внимание на том, что СМИ имеют большое влияние на общество и являются его неотъемлемой частью на данном этапе развития технологий. Также СМИ могут оказывать как положительное, так и отрицательное влияние на формирование мировоззрение человека.

Список используемых источников:

1. Комаровский, В.С. Управление общественными отношениями [Текст]: Учебник / под общ. редакцией А.С.Комаровского. - М.: Манускрипт, 2006.- 400 с.
2. Фетов Д.М. Манипуляция сознанием [Текст]: Д.М.Фетов // Человек и наука, 2008. - № 7 . - 5-10.
3. Научно-практические конференции ученых и студентов. Публикации Scopus и Web of Science. Авторские и коллективные монографии. Режим доступа: https://sibac.info/studconf/social/xiv/35007. Дата обращения: 17.11.2017.
4. Общество и СМИ. Режим доступа: http://videoforme.ru/wiki/rol-smi-v-obshhestve. Дата обращения: 20.11.2017.

5. Особенности влияния средств массовой информации на формирование общественного сознания. Режим доступа: http://diplomba.ru/work/80471. Дата обращения: 15.11.2017.
6. Средства воздействия СМИ на общественное сознание в условиях информационного общества
7. Гаврилов А. А. Средства воздействия СМИ на общественное сознание в условиях информационного общества // Молодой ученый. — 2012. — №8. — С. 152-155. Режим доступа: https://moluch.ru/archive/43/5220/. Дата обращения: 20.11.2017.
8. Компьютерные игры как новый вид политических технологий. Режим доступа: http://politinform.su/nacionalnaya-bezopasnost/44162-kompyuternye-igry-kak-novyy-vid-politicheskih-tehnologiy.html. Дата обращения: 15.11.2017.
9. Учебники онлайн. Основные технологии воздействия на общественное сознание СМИ. Режим доступа: http://uchebnik-online.com/131/1155.html. Дата обращения: 15.11.2017.

СЕКЦИЯ 2. «СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ «УМНЫХ» ОБЪЕКТОВ»

«УМНЫЕ» СЕТИ ДЛЯ ВЫСОКИХ ТЕХНОЛОГИЙ

(ПРОЕКТ SMART GRID)

Попов Алексей Андреевич
ОГБПОУ «Кожевниковский техникум агробизнеса»
Руководитель: Морозов И.В.

Введение

В настоящее время встает все больше проблем, связанных с качественным и количественным обеспечением электроэнергией. Возникает необходимость принятия быстрых и эффективных решений, которые смогли бы вывести мировую энергетику на совершенно новый уровень развития. В этой связи в электроэнергетике имеют место следующие задачи: обеспечение потребителей достаточным количеством высококачественной электроэнергии, минимизация затрат на производство и передачу энергии, оперативное реагирование на любые изменения в сети, использование в процессе производства энергии возобновляемых экологичных ресурсов. На данный момент западными специалистами разработана и активно внедряется технология Smart Grid, позволяющая решить поставленные задачи.

Технология Smart Grid: зарубежный и российский опыт

Интеллектуальные энергосистемы (Smart Grid) – это автоматизированная система, самостоятельно отслеживающая и распределяющая потоки электричества для достижения максимальной эффективности использования энергии. Использование современных информационных и коммуникационных технологий, позволяет взаимодействовать оборудованию сети Smart Grid друг с другом, образуя единую интеллектуальную систему энергоснабжения. Со-

бранная с оборудования информация анализируется, а результаты анализа помогают оптимизировать использование электроэнергии, снизить затраты, увеличить надежность и эффективность энергосистем.

Рис. 1. Схема, иллюстрирующая систему взаимодействия в рамках проекта «SmartGrid»

Основой интеллектуальной сети являются информационно-коммуникационные технологии. Предпосылками для образования таких сетей являются следующие технологии и свойства: системы скоординированного управления и распределенной автоматизации и контроля, распределенный интеллект устройств, интеграция системы управления с операционными устройствами и коммуникация замеренной даты для целей управления, и принятия решений. для обеспечения работы Smart Grid, энергосистема должна иметь программное обеспечение, созданное на основе методов искусственного интеллекта. Интеллектуальный учёт позволяет осуществлять передачу данных о количестве потреблённой электроэнергии в режиме реального времени. Счётчики такой системы способны отследить данные по каждому бытовому устройству и установить определённые правила работы в часы максимальных нагрузок. Интеллектуальные счетчики электроэнергии – так называемые «смарт метры» – позволяют оценивать расход энергии и передавать данные оператору и потребителю по сотовой связи, Wi-Fi и другим беспроводным каналам связи. Счетчики электроэнергии можно запрограммировать на коммуникацию с различной бытовой техникой и управлять ей с учетом различных условий тарификации. Интеллектуальные счетчики позволяют обнаруживать потери

энергии в сетях, облегчая, таким образом, поиск и устранение дефектов на линии.

Также “умная” сеть Smart Grid обладает рядом преимуществ:

1. Надежность и качество электроснабжения

Smart Grid предотвращает массовые отключения, обеспечивает поставку чистой электроэнергии.

2. Безопасность

Smart Grid постоянно контролирует все элементы сети с точки зрения безопасности их функционирования.

Здесь можно вспомнить о таких проблемах с энергоснабжением в Московской области, когда в зимнее время в связи с погодными условиями происходило обледенение линий электропередач, так и о проблемах в Москве жарким летом в связи с пожарами на высоковольтных подстанциях.

3. Энергоэффективность

Снижение потребления электрической энергии. Оптимальное потребление приводит к снижению потребностей в генерирующих мощностях.

4. Экология и охрана окружающей среды

Самый главный эффект достигается за счет снижения количества и мощностей генерирующих элементов сети. Это ведет, например, к снижению выброса CO в атмосферу.

5. Финансовые преимущества

Снижение операционных затрат. Потребители имеют точную информацию о стоимости и могут оптимизировать свои затраты на электрическую энергию. Бизнес, в свою очередь, может оптимально планировать и формировать затраты на эксплуатацию и развитие генерации и распределительных сетей.

Владельцы «Умного дома» смогут управлять своим жилищем дистанционно, с помощью iPad или другого электронного устройства через специальную вебстраницу. Управление приборами учёта на расстоянии, позволит энергетическим компаниям увеличить эффективность распределения между потребителями электроэнергии и сократить до минимума кражи электроэнергии, а также

эффективнее бороться со злостными неплательщиками. Динамическое управление сетями позволяет подключить к интеллектуальной сети всё оборудование электросетевого хозяйства, в результате чего, единый центр будет видеть текущее состояние устройств, не покидая главного офиса в любой момент времени. Это позволит более оперативно реагировать на аварии и сбои в системе. Система Smart Grid регулирует спрос, перераспределяя его по времени суток. Использование всех энергопотребляющих устройства в дневное время, усиливает нагрузку на сеть, Smart Grid предлагает часть из них запускать в работу в ночное время – часы минимальной нагрузки, выравнивая тем самым, график нагрузки на сеть. Система интеллектуального учёта подразумевает под собой безопасный обмен данными. Потребитель должен быть уверен в том, что данные о его количестве использованной энергии не будут «перехвачены» злоумышленниками, не будет искажена, и что никакое «третье лицо» не вмешается в процесс информационного обмена. Интеллектуальная IP-сеть во многом решает вопросы как информационной, так и физической безопасности. Интеллектуальные сети Smart Grid из-за непрерывного мониторинга использования энергии, позволяющего потребителю более точно прогнозировать и контролировать своё энергопотребление, в значительной степени его дисциплинирует и, тем самым, положительно влияет на энергосбережение в целом. Задача для электросетевого комплекса интеллектуализации сети является одной из важнейших. Сейчас уже реализуются проекты внедрения интеллектуальных систем учёта потреблённой энергии, однако, при нынешних проблемах ввода подобных систем, данный процесс идёт медленными темпами.

В настоящее время Smart Grid эффективно применяются за рубежом. В некоторых штатах США проводились исследования по вводу «интеллектуальных» сетей. В результате снизились пиковые нагрузки на электросеть. В среднем на 10 % уменьшились счета за электричество, при этом его стоимость увеличилась на 15 %. С 2007 года создание системы Smart Grid – стала одним из национальных приоритетов Соединенных Штатов. по некоторым

оценкам использование системы Smart Grid к 2020 году позволит США сэкономить около 1.8 трлн. долл. за счет снижения потребления энергии и повышения надежности.

Интенсивность инвестиций Китая в интеллектуальную энергетику позволяет экспертам прогнозировать, что в ближайшее десятилетие КНР выйдет в лидеры по темпам роста рынка компонентов Smart Grid. При нынешней динамике развития этого сегмента прогнозируется, что в период 2011-2021 годов он достигнет уровня среднегодового роста в 6 % до 1,43 трлн долларов. КНР в таком случае объективно обойдет США, где на сегодняшний день этот показатель составляет 4 %. В результате Китай может выйти на передовые позиции и стать мировым лидером на рынке Smart Grid.

В России наблюдается повышенный интерес к рассматриваемой технологии, неслучайно приоритетным развитием науки, технологий и техники в Российской Федерации признано направление «Энергоэффективность, энергосбережение». В 2008 году был подписан Указ Президента «О некоторых мерах по повышению энергетической и экологической эффективности российской экономики», в котором сформулирована цель снизить к 2020 году энергоемкость ВВП РФ не менее чем на 40 % по сравнению с 2007 годом. Одним из первых городов РФ, в котором была внедрена система Smart Grid, стал город Белгород, вошедший в общемировой проект «Умный город». В ряде распределительных сетей Белгорода установлены специальные устройства, которые помогают с большой точностью определить место разрыва проводов и отключить в данном случае только небольшое количество потребителей электроэнергии. Так же в городе действует «умное освещение», контролирующее энергопотребление, состояние сетей, число работающих ламп. Система поэтапно управляет уличным освещением в зависимости от условий видимости и количества людей на улицах.

По мнению экспертов, на первом этапе внедрения Smart Grid в России возможна реализация только принципов наблюдаемости, автоматизации. Это

означает, что, в первую очередь, будут внедрены информационные технологии (автоматический учет, телемеханика, системы защиты и т.п.). Далее – цифровые подстанции. Для сети Smart Grid в России имеются достаточные предпосылки. Следует отметить исследования отечественных ученых в области теории управления большими энергетическими системами и кибернетики энергосистем, ряд положений и результатов, которые применяются в зарубежной идеологии преобразования электроэнергетики. В то же время имеются объективные сдерживающие факторы внедрения Smart Grid: степень развития информационных технологий, силовой электроники, альтернативных источников электроэнергии. Неоправданно заниженная стоимость электроэнергии для бытового потребления и неготовность бытового потребителя к планируемой либерализации трафика. Высокий уровень потерь в сетях. Растущее несоответствие требования международного сообщества в части охраны окружающей среды.

Интересен опыт г. Уфы, который попал в «умные сети». С 2013 года в столице Башкортостана реализуется совместный проект компании «Сименс» и АО «БЭСК» по модернизации электросетевого комплекса. В рамках этого проекта в ближайшие годы город полностью перейдет на интеллектуальное управление сетями. Предстоит обновить 512 наблюдаемых и 157 управляемых трансформаторных пунктов, а также проложить 350 км кабельных линий.

На первом этапе проекта был модернизирован жилой микрорайон Зеленая Роща с населением 25 тысяч жителей. Кроме того, заработал новый Центр управления сетями (ЦУС), куда стекается вся информация с объектов. Здесь находятся не только диспетчеры, но и сопровождающие их работу службы, серверы, а также учебные классы. Центр управления сетями объединяет восемь диспетчерских пунктов города и обеспечивает полный мониторинг нагрузки и режимов электросетевого оборудования.

Smart Grid – это не просто технология, а целая философия, где главное – получение информации с ее последующей обработкой. В случае аварийной ситуации происходит обмен информационными сигналами между устройствами,

сразу после этого диспетчер видит место повреждения на электронной схеме в центре управления. Программа сама предлагает варианты обхода неисправного участка. Проходит всего две минуты с момента аварии, а питание микрорайона уже восстановлено.

Помимо наблюдения за сетью, диспетчеры отслеживают и действия бригад, выезжающих в случае необходимости на энергообъекты. Ведь каждая машина оборудована модулем ГЛОНАСС. Такой подход позволяет автоматически просчитывать статьи расходов, формируя бюджет на оперативно-техническое управление.

Для того чтобы повысить качество электроснабжения, снизить затраты и потери энергии, «Сименс» использовал в уфимском проекте такие технологии:

- устройства контроля состояния сети, которые позволяют обнаружить короткое замыкание и указать его направление, а также контролировать основные электрические параметры);
- оборудование релейной защиты и автоматики серии SIPROTEC Compact, обеспечивающий защиту, автоматику и управление распределительными устройствами;
- контроллеры SICAM TM, которые собирают сигналы о положении ключей, коммутационных аппаратов и о срабатывании системы защиты, а также передают команды на управление.

Для переоснащения энергетических объектов также применяется высокотехнологичное оборудование «Сименс», сборочное производство которого уже локализовано в регионе. Речь идет о комплектных распределительных устройствах среднего напряжения с электрогазовой изоляцией (КРУЭ), устанавливаемых на распределительных и трансформаторных подстанциях. Оборудование позволяет осуществлять дистанционное управление, а также передачу сигналов телеизмерений и телесигнализации от подстанций к диспетчерскому центру.

Элементы «умных сетей» помогают обнаружить и несанкционированные подключения. По расхождению показаний счетчиков несложно вычислить место такого подключения, чтобы оперативно принять меры. В конце 2014 года потери электроэнергии в целом по Уфе составляли порядка 16–17%. По окончании проекта, к 2020 году, этот показатель снизится в два раза.

Выводы

Таким образом, внедрение интеллектуальной энергосистемы в нашей стране, несомненно, связано с техническим прорывом в области коммуникаций, технологических решений по развитию альтернативных источников энергии, разработкой моделей и алгоритмов функционирования энергосистемы на основе методов искусственного интеллекта. К тому же развитие отрасли ИКТ (информационно-коммуникационных технологий) простимулирует инвестиции в такие решения, которые повысят надежность электроснабжения, уменьшат эксплуатационные расходы системы и обеспечат безопасность функционирования.

Список используемых источников:

1. http://www.sicon.ru/about/articles/?base=&news=16
2. http://www.smartgrid.su/2010/02/18/umnaya-set/
3. Ледин С.С., Игнатичев А.В. Развитие промышленных стандартов внутри- и межсистемного обмена данными интеллектуальных энергетических систем // Автоматизация и IT в энергетике. – 2010. – № 10
4. Концепция энергетической стратегии России на период до 2030 года (проект). Прил. к журналу «Энергетическая политика». – М.: ГУ ИЭС, 2007.
5. Бударгин О. Умная сеть – платформа развития инновационной экономики. – Круглый стол «Умные сети – Умная энергетика – Умная экономика», Петербургский международный экономический форум, 17 июня 2010 г.
6. Дорофеев В.В., Макаров А.А. Активно-адаптивная сеть – новое качество ЕЭС России // Энергоэксперт. – 2009ю – № 4 (15).

«ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ДИСТАНЦИОННОГО УПРАВЛЕНИЯ ОБЪЕКТОМ. ПРЕИМУЩЕСТВА И УЯЗВИМОСТЬ СИСТЕМ «УМНОГО» ДОМА»

Карпов Степан Сергеевич
ОГБПОУ «Томский коммунально-строительный техникум»
Руководитель: Головнева Анастасия Владимировна

Введение

Принято считать, что концепция «Умного дома» (от английского *smart house*) берет свое начало в середине прошлого века, но из-за высокой стоимости реализации подобные проекты не получили широкого распространения. Ситуация в корне изменилась с развитием электроники и в настоящее время такие системы хоть все еще не внедряются повсеместно, но уже и не воспринимаются как диковинка.

Гипотеза. «Умные» объекты облегчают повседневную жизнь человека, но в то же время они не могут гарантировать 100% информационную защиту владельца.

Проблема исследования. Проблема уязвимости интеллектуальных систем дистанционного управления объектом.

Актуальность настоящей темы обусловлена, с одной стороны, большим интересом к теме автоматизированных систем, с другой, недостаточной защищенностью этих систем в информационном пространстве.

Целью исследования является изучение всех преимуществ и возможных недостатков систем «умного дома».

Задачи исследования:

1. Изучить возможности и недостатки систем «умного» дома.
2. Проанализировать актуальность системы «умный дом» или smart home, в России и за рубежом.

Методы исследования

1. изучение и анализ материалов сети Internet;

2. системный анализ запросов в поисковой системе Google trends, по интересующей нас теме.

Немного истории

Первым полноценным проектом «умного дома» в 1980-х годах стал небольшой жилой дом на южном берегу Англии. В основу его автоматики легло использование широкополосной KNX-системы, отвечающей за управление освещением, сигнализацией, жалюзи, отоплением и дверями гаража. Также в данном доме был создан бассейн, который впоследствии дополнили LED-системой с оригинальными цветовыми эффектами.

Современные системы ушли далеко вперед, существенно расширив свои технические возможности. Сегодня в них используются встраиваемые домашние кинотеатры, объединяются все инженерные системы, применяется интеллектуальное управление на основе специального программного обеспечения (ПО). Благодаря модульности системы у пользователей появилась возможность самостоятельно выбирать функционал «умного дома».

Что включает в себя система «умного» дома?

Система «Умный дом» — это высокотехнологичная система, позволяющая объединить все коммуникации в одну и поставить её под управление искусственного интеллекта, программируемого и настраиваемого под все потребности, и пожелания хозяина.

«Умный дом» — единая система управления в доме, офисе, квартире или здании, включающая в себя датчики, управляющие элементы и исполнительные устройства. Управляющие элементы принимают сигналы с датчиков и контролируют работу исполнительных устройств, действуя согласно заданным алгоритмам и объединяя следующие системы:

- Отопление дома (посредством радиаторов или теплых полов)
- Вентиляция и кондиционирование
- Охранная и пожарная сигнализация
- Система контроля доступа

– Контроль аварийных ситуаций: утечки воды, газа, аварии в электросети

– Видеонаблюдение (локальное и удаленное)

– Управление внутренним и уличным освещением

– Распределение видео и аудиопотоков по помещениям (мультирум)

– Управление обогревом ливневой канализации, ступеней лестниц и дорожек

– Контроль над энергопотреблением, ограничение пиковых нагрузок и распределение нагрузок по фазам питающей сети

– Управление источниками резервного электропитания: аккумуляторными и дизель-генераторами

– Управления канализационных насосных станций и системам автополива зеленых территорий

– Управление воротами и шлагбаумами

– Управление шторами, рольставнями и жалюзи

– Удаленный мониторинг и управление всеми системами дома через интернет.

Как видите, возможности системы «умного» дома практически безграничны и могут быть полезны как для загородного дома или гаража, так и для организации обслуживания огромных комплексов.

Конечно, совсем без человека такая система не функционировала бы, но его роль ограничивается настройкой программного обеспечения и контроля ее работы, в том числе и удаленно – это и является одним из главных преимуществ подобных систем.

Проблемы безопасности «умных» систем.

«Умный» дом включает в себя огромное количество IoT-устройств, собирающих и обрабатывающих данные. Они дают пользователям определённые возможности по контролю за апартаментами как в ручном, так и автома-

тическом режиме. Из-за того, что все элементы цепочки имеют доступ в Интернет, это делает их уязвимыми к атакам извне и подвергает опасности личную информацию пользователя.

Компания HP провела исследование рынка интеллектуальных систем в ходе которого выяснила, что практически все системы имеют проблемы с безопасностью.

Первая проблема – недостаточно надежная проверка подлинности. Системы, несмотря на то, что обладали облачными и мобильными интерфейсами, не требовали установки паролей достаточной длины и сложности. Также ни одна из систем не блокировала учетную запись после определенного числа неудачных попыток ввода пароля – получается, что отсутствовала банальная защита от перебора.

Еще одна проблема оказалась связана с конфиденциальностью. Все системы собирали какие-либо виды персональной информации: имена, адреса, номера телефонов и кредитных карт. Это вызывает определённую озабоченность, поскольку создает угрозу кражи учетных данных.

Стоит также отметить, что ключевой особенностью многих домашних систем безопасности является использование видео, просмотр которого доступен через различные интерфейсы. Конфиденциальность подобных данных тоже находится под вопросом.

Наконец, последней проблемой эксперты назвали отсутствие шифрования при передаче данных. Хотя во всех системах реализованы механизмы шифрования на транспортном уровне, но многие облачные подключения остаются уязвимыми для атак.

А это очень важный момент: чтобы исключить несанкционированное вмешательство в работу устройства, обмен между контроллером и сервером должен идти в зашифрованном с помощью ключа виде.

К счастью, уже многие компании с известными мировыми именами, такие как: *Google, Samsung Electronics, Silicon Labs* и некоторые другие объединились с целью разработать новый беспроводной сетевой стандарт специально

для «умных» домов. Он получил название *Thread*. Основным его достоинством является именно безопасность. Одновременно в сети могут находиться до 250 устройств, которые защищаются шифрованием уровня банковской системы.

Еще одна особенность *Thread* – это прозрачность. Пользователь видит список всех подключенных устройств, благодаря которому ему легко определить, что с чем связано. В настоящий момент есть ряд решений для умных домов (*ZigBee* и *6LowPAN*), которые легко могут начать поддерживать предложенный стандарт без аппаратных изменений – в их случае нужно просто обновить программное обеспечение.

Анализ статистических данных сервиса Google Trends

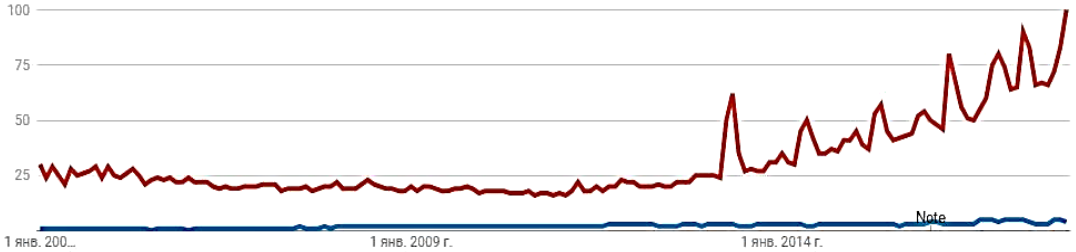
Свое дальнейшее исследование мы продолжим вместе с *Google Trends* – это сервис, позволяющий просматривать тренды по поисковым запросам *Google* начиная с далекого 2004 года.

Чем интересен данный ресурс и полезен для нас? Во-первых, мы имеем возможность просматривать статистику запросов за разный период времени, во - вторых, запрашивать данные по всему миру или отдельным странам. Рассмотрим оба варианта, чтобы иметь возможность анализировать актуальность темы «умных» домов в нашей стране на ряду с другими развивающимися странами.

Для того, чтобы проследить динамику интереса выбранной темы, мы будем работать со статистикой за максимально длинный период, за 13 лет, и так как мы хотим сравнить актуальность «умных» систем в России и за рубежом, то будем сравнивать два запроса:

1. «Умный» дом
2. Smart home

Сравнивая эти два запроса, мы видим существенную разницу в кривизне диаграмм *(рис. 1)*. Из этого можем делать вывод, что за рубежом данные системы наиболее интересны обывателю, нежели чем в России. Возможно, это от части потому, что в Америке первые «умные» устройства существовали в 1960х годах, а в Россию они пришли только к 80м годам прошлого века.



«умный дом» – синяя кривая *«smart home»* – красная кривая

Рис. 1. Динамика популярности запросов «умный дом» и «smart home» по всему миру, в поисковой системе Google с 1 января 2004 года.

А если к данной диаграмме мы подключим географическую аналитику данных запросов, то наглядно продемонстрируем актуальность темы по всему миру *(рис. 2.)* и наиболее активных городах и странах *(рис. 3.)*.

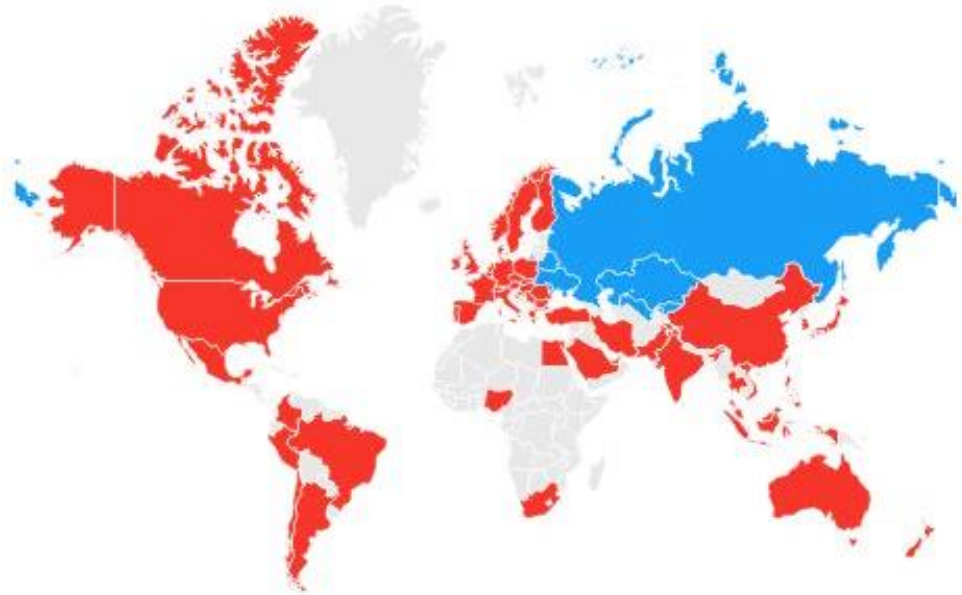


Рис. 2. Популярность запросов «умный дом» и «smart home» по Регионам

Рис. 3. Популярность запросов «умный дом» и «smart home» по городам и странам, в поисковой системе Google с 1 января 2004 года

Если же посмотреть на график запросов «умный дом» в России с января 2004 года, то мы увидим, что интерес к данной теме с мая 2008 года, по январь 2017 стабильно падал и лишь последний год пошел на подъем *(рис. 4.)*. Я думаю, это связано с тем, что люди чаще стали задумываться об эффективности энергопотребления, своей безопасности.

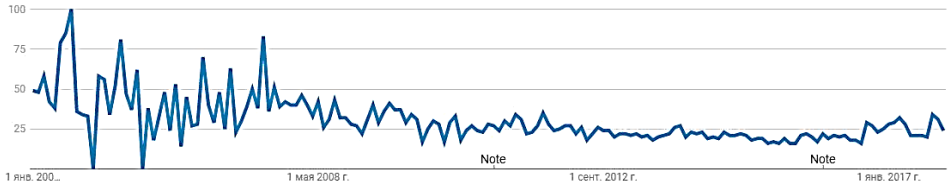


Рис. 4. Динамика популярности запроса «умный дом» в России, в поисковой системе Google с 1 января 2004 года

Рассматривая более подробно данный запрос, например, за последний год, мы увидим, что диаграмма более стабильна, а интерес к данной теме повышается в холодные месяцы *(рис. 5.)*. Думаю, основной причиной данной статистики является вопрос эффективности энергосбережения. Ведь, действительно, это одно из основных направлений «умных» систем.

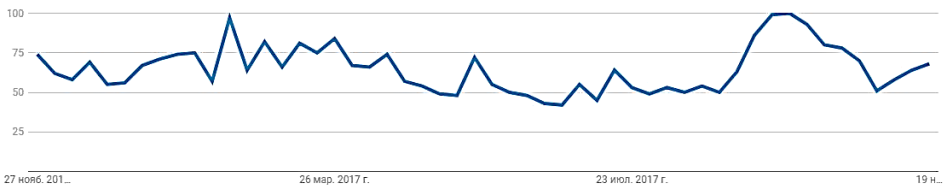


Рис. 5. Динамика популярности запросов «умный дом» за 2017 год

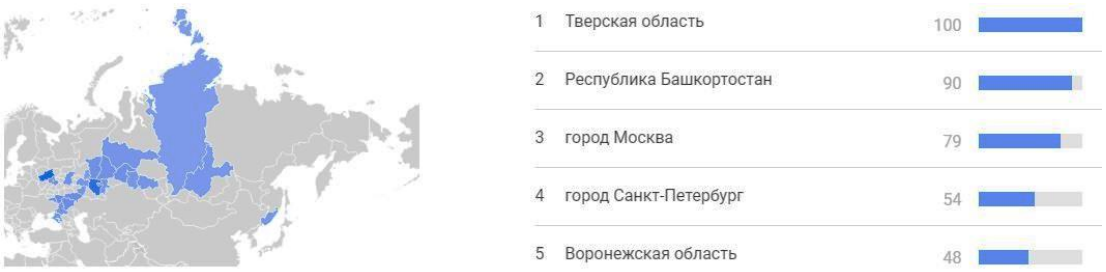


Рис.6. Популярность запросов «умный дом» по субъектам РФ за 2017 год

Анализ литературы по теме исследования

При выполнении данной работы я использовал только интернет-ресурсы, потому как печатной литературы по данной теме не нашел. Дефицит печатных изданий по выбранной теме говорит о новизне и актуальности данного исследования.

Выводы

Очевидно, что присутствие в нашей жизни «умных» объектов облегчает нам жизнь и делает ее комфортнее. Но мы должны понимать, что на ряду с многочисленными плюсами, имеются и недостатки подобных систем, такие как дороговизна и недостаточная информационная защищенность обладателей «умных» объектов.

И несмотря на сложность данной системы, основываясь на статистике, можно смело утверждать, что данная тема актуальна и до конца не изучена, что позволяет и дальше продолжать исследование как в области информационных технологий, так в области строительства и бизнеса.

Работа рассматривает лишь один из аспектов проблемы. Исследования в данном направлении могут быть продолжены. Это могло бы быть изучение не только проблем уязвимости систем дистанционного управления объектом, но и создание подобных систем своими руками, что позволило бы снизить стоимость «умных» объектов.

Данная работа будет интересна студентам старших курсов СПО или ВУЗов многих специальностей, которые задумываются о выборе темы для дипломного проектирования, или ищут идею для дальнейшей профессиональной деятельности.

Список используемых источников:

1. http://www.dom-electro.ru
2. https://bonavilla.ru
3. https://dimdom.ru/tehnologiya-umnyy-dom-svoimi-rukami-chto-eto-takoe.html
4. https://www.asutpp.ru/elektrika-v-kvartire/sistema-umnyj-dom.html
5. https://kopilkaurokov.ru/informatika/presentacii/priezientatsiiapotiemieumnyidom
6. http://research.ifmo.ru/ru/news2/5832/bezopasnyy_umnyy_dom:_slozhnaya_tehnologiya,_poleznaya_kazhdomu.htm
7. https://news.rambler.ru/europe/35883588-umnye-doma-budut-preduprezhdat-o-sboe-kriticheskih-sistem/
8. http://easyen.ru/forum/26-380-2
9. https://geektimes.ru/company/gsgroup/blog/276006/

АНАЛИЗ ВОЗМОЖНЫХ УЯЗВИМОСТЕЙ СИСТЕМ «УМНОГО ДОМА»

Геращенко Егор Владимирович
ОГБПОУ «Томский техникум информационных технологий»
Руководитель: Королев Елена Евгеньевна

Введение

Актуальность. В данной исследовательской работе мы хотели бы обсудить такую проблему, как уязвимость “умных” объектов. Эта проблема очень актуальна во всех сферах жизни современного общества. Информационные технологии развиваются стремительно и постепенно занимают все больше места в нашей повседневной жизни. К примеру, существуют системы дистанционного управления бытовой техникой, когда пользователь задает приборам список нужных действий и время их исполнения. Вроде бы, сегодня это не удивительно – но тут речь идет лишь о нескольких независимых друг от друга электронных устройствах. А если взять целую систему таких устройств, которые, как живой организм, будут управлять температурой в помещениях, их водоснабжением, охраной, проветриванием и многими другими факторами? Это будет совершенно иной уровень управления, комплексный! Безусловно, такая система будет нуждается в защите от различных неполадок и попыток взлома. Давайте попробуем разобраться в этом вопросе подробнее.

Цели и задачи исследования. Целью нашего исследования является рассмотрение и анализ системы “Умный дом”, все тонкости этой системы, её преимущества и недостатки, методы обслуживания. Задачей будет подтверждение или опровержение жизнеспособности «умного дома».

Гипотеза исследования. Какими бы эффективными и полезными не были “умные” здания, они до сих пор не завоевали большую аудиторию. Как и прежде мы живем в привычных домах, где самостоятельно обеспечиваем себе необходимый уровень комфорта, улучшая его качество использованием

некоторого количества разноплановой бытовой техники. Получается, что “умные” здания не так уж и востребованы? А нужны ли они нам вообще?

1. Умный дом

Наверное, каждый мечтает, чтобы по приходу с работы, его встретил и окутал комфортом интеллектуальных и инженерных удобств его «умный» дом. При входе в гостиную включались бы мягкий свет и телевизор. Ванна сама собой наполнялась бы водой нужной температуры, включался бы обогрев пола и система вентиляции. Было бы здорово, если после ухода хозяина на работу, умный дом сам брал бы себя под охранную сигнализацию, а при нестандартных ситуациях оповещал бы хозяина по мобильной связи.

Давайте для начала попробуем понять, что же такое «умный дом» и «умные здания» в целом.

«Умный дом» – это единая система контроля и управления системами жизнеобеспечения и комфорта, в квартирах, офисах или целых зданиях, включающая в себя датчики контроля, элементы управления и исполнительные устройства. Есть много различных определений понятия «интеллектуального здания», но все они имеют общую концепцию: это система, структура, управление и обслуживание.

Основаны такие технологии на компьютерной информационной системе, которая и дает определение термину «интеллектуальное здание». Эта система самостоятельно собирает и анализирует ситуационную информацию с различных датчиков и формирует управляющие сигналы в соответствии с заданными алгоритмами

Поэтому можно утверждать, что здание становится «умным» только при наличии множества связанных между собой подсистем управления, которые подчинены единому общему центру. Наличие в здании некоторого числа разрозненных компьютерных систем еще не делает его «умным». Подобное название применимо лишь тогда, когда все подсистемы в здании будут общаться друг с другом через централизованную контролирующую и координирующую информационно-компьютерную систему.

2. Работа системы

В настоящее время технология «интеллектуального здания» включает в себя около тридцати различных систем: управление локальной сетью, доступ в интернет, телефонная связь, подача горячей и холодной воды, электропитание, вентиляция и кондиционирование, управление лифтами.

Слаженность работы всех этих подсистем обеспечивается алгоритмами управления, которые «умная» система запускает в той или иной ситуации.

Например, при отсутствии в здании людей, система анализирует информацию от датчиков движения, температуры, освещения, ударов, утечки, протечки и т.д. – и запускает алгоритмы экономного расходования энергии, повышая тем самым безопасность путем отключения света, перекрытия подачи воды, перевода климатической системы в экономный режим и т. п.

Другой пример – в здание проник посторонний человек. Сценарий безопасности будет основан на сборе информации с датчиков теплового излучения, датчиков движения, уровня воспроизводимых шумов в помещении, магнитных дверных контактов, внешних и внутренних стационарных и поворотных видеокамер, систем сигнализации и целостности жилища. Эти датчики постоянно контролируют состояние различных зон дома и, в зависимости от происходящих изменений, передают сигналы в систему. Когда система безопасности фиксирует определенный сигнал, то запускает соответствующий ситуации алгоритм (закрытие механических оконных ставней, блокирование дверей, включение звукового оповещения или подача мигающих световых сигналов).

Основное назначение этих мер – блокирование нарушителя и информирование хозяина дома о возникшей угрозе, либо передача сигнала тревоги на центральный охранный пункт.

3. Составляющие системы

В состав «интеллектуального» здания входят:

- **комплекс технических средств безопасности:**

- система централизованного сбора и обработки информации;

- система телевизионного наблюдения и контроля;
- система тревожно-охранной сигнализации;
- система управления доступом в помещение;
- система пожарной сигнализации и оповещения о пожарной опасности;
- система автоматического пожаротушения.

➢ **комплекс систем жизнеобеспечения:**

- система бесперебойного гарантированного электроснабжения;
- системы кондиционирования воздуха, вентиляции и отопления;
- система управления микроклиматом в помещениях;
- системы управления освещением и системы освещения;
- система удаленного наблюдения и управления электроснабжением;
- система учета энергоносителей;
- системы контроля и управления эскалаторами, лифтами, и т.д.

➢ **комплекс систем информатизации:**

- локальная компьютерная сеть;
- система приема спутникового и эфирного телевидения;
- система радиофикации;
- система телефонной сети;
- система проведения конференций;
- система контроля и координации времени;
- средства оперативной радиосвязи для персонала.
- структурированная кабельная система;
- единый диспетчерский центр

4. Преимущества комплексных систем «интеллектуальных зданий»

Концепция «интеллектуальных зданий» (ИЗ) предназначена для настройки ее на индивидуальные потребности заказчика. Используемые в них «интеллектуальные» системы управления позволяют обитателям таких зданий получать настроенные на индивидуальные требования комфорт, безопасность, эффективное использование оборудования, получение сведений о состоянии

систем в здании. В итоге получаем снижение эксплуатационных затрат на потребление энергоресурсов и воды, а также оптимальный режим эксплуатации оборудования.

В «интеллектуальных зданиях» оптимизированы основные элементы "среды обитания" и взаимоотношения между ними (структура, системы, управление, службы). Эксперты подсчитали, что применение таких комплексных интегрированных систем позволяет экономить от 15% и выше затрат владельцев на установку оборудования путем устранения излишних связей в инфраструктуре здания. Меньше затрат потребуется и на обучение персонала управлению «умным» комплексом. Хозяин дома получает возможность управлять всеми системами объекта с одного централизованного персонального компьютера.

Комплексная система имеет следующие преимущества в сравнении с разрозненными автономными системами:

- значительная экономия на сетевом оборудовании и кабельных сетях;
- повышение надежности всей системы и снижение энергопотребления;
- повышение оперативности управления объектом в целом;
- графическое предоставление информации о состоянии оборудования и систем на различных уровнях (зональном, объектовом, адресном);
- снижение трудозатрат диспетчерских и эксплуатационных служб;
- обеспечение требуемого взаимодействия подсистем;
- снижение вероятности возникновения неисправностей и «страховых случаев»;
- открытость систем комплекса, дающая возможность его модернизации и наращивания, а также использования оборудования от разных производителей.

На строительство ИЗ потребуется, конечно, больше материальных ресурсов, чем на здания с привычным нам инженерным оборудованием. Но при этом надо помнить, что совокупная стоимость здания – это сумма затрат не

только на строительство, но и на его эксплуатацию в течение всей жизни здания. По оценочным данным на сегодня усредненная стоимость эксплуатации зданий в России в десятки раз превышает стоимость их постройки. Поэтому можно сделать вывод, что большую часть денег мы тратим именно на эксплуатацию зданий, а не на их создание. Сегодня в Европе наметилась противоположная тенденция: больше денег вкладывать в строительство, для того чтобы потом существенно экономить на периоде эксплуатации здания. Возможно, имеет смысл и нам последовать этому примеру?

Формирование в здании инженерной инфраструктуры типа «умного дома» серьезно повысит его ликвидность. Комплекс ИЗ будет являться эффективным инвестиционным решением, позволяющим серьезно сократить расходы на обслуживание и развитие зданий. Такие здания будут соответствовать современным международным стандартам и станут привлекательным рыночным предложением.

5. Недостатки систем «интеллектуальных зданий»

Одним из главных недостатков технологий ИЗ все-таки является их сравнительно высокая стоимость, даже несмотря на последующую экономию средств при эксплуатации.

Также экспертами были проведены исследования и испытания некоторых из наиболее популярных устройств «умного дома». Была выявлена их уязвимость для хакерских атак. При доступе к управлению на большинстве этих устройств не заложено требование задания паролей достаточной длины и сложности. Также многие из этих устройств не используют шифрование при передаче данных. Были выявлены около десятка смарт-продуктов, подверженных опасности: веб-камеры, smart TV, удаленные розетки, «умный» термостат, дверные замки, система открывания гаражной двери, системы полива участка, напольные весы, домашняя сигнализация, сетевой концентратор. для управления сразу несколькими устройствами. Наиболее уязвимым моментом для этих устройств стало отсутствие требования о сложном пароле для входа в систему. В большинстве случаев использовались такие простые пароли, что их можно

было вычислить простыми методами подбора. Интерфейсы, используемые на сайтах шести смарт-устройств, также не отвечают требованиям безопасности и могут привести к утечке информации. Хакеры используют средства для сброса пароля и имеют шанс получить доступ к счетам и конфиденциальной информации пользователей ИЗ. Также поводом для беспокойства является отсутствие шифрования для защиты цифровых данных от несанкционированного прочтения при передаче. Этим тоже могут воспользоваться хакеры и перехватить, модифицировать и повторно ввести код, что грозит опасностью утери контроля над оборудованием, программным обеспечением и данными «умного дома». Многие устройства собирают и накапливают личную конфиденциальную информацию (имя, адрес, дату рождения, серии и номера медполисов и кредитных карт). Многократно возрастает опасность утечки такой информации при использовании облачных сервисов и мобильных приложений смарт-устройств. Передача незашифрованной информации через домашнюю сеть делает возможным несанкционированный доступ к ней через беспроводные сети.

Заключение

На основании вышеизложенного можно сделать следующий вывод: “умные дома” представляют собой перспективное направление развития рынка недвижимости и IT-технологий. Но в техническом аспекте эта отрасль пока достаточно уязвимая для хакерских атак, она имеет большое число недостатков и проблем, над которыми предстоит еще много работать. Но, несмотря на сегодняшние недостатки, интегрированные системы «умных зданий», вполне возможно, станут частью нашей повседневной жизни в будущем. При этом должна также появиться и сфера подготовки конечных пользователей таких систем, несмотря на всю кажущуюся простоту в их управлении. Человек будущего, чтобы жить в «умном доме», должен понимать его, а для этого – иметь достаточные знания в IT-сфере. Следовательно, образование должно сместиться в сторону свободного владения компьютерными технологиями, такую же как уметь читать и писать.

Список используемых источников:

1. Гололобов, В. Н. «Умный дом» своими руками НТ Пресс, 2012. – 416 с.;

2. В. А. Тётушкин, Б. И. Герасимов «Система управления интеллектуальным зданием как инновационный элемент сервиса недвижимости» [Электронный ресурс] http://vernadsky.tstu.ru;

3. В.И.Репин «Интеллектуальное здание» [Электронный ресурс] http://www.i-home.ru;

4. Официальный сайт компании HDL RUS «Интеллектуальное здание» [Электронный ресурс] https://hdlrus.ru;

5. Официальный сайт компании ТОМСК-ЭНЕРДЖИ «Умный дом» [Электронный ресурс] http://tomskenergy.ru;

6. Официальный сайт компании INTEL «Решения Intel® для умных зданий» [Электронный ресурс] https://www.intel.ru;

7. Официальный сайт компании dom-electro «Что такое Умный дом?» [Электронный ресурс] http://www.dom-electro.ru/

«УМНЫЙ» ДОМ. МЕТОДЫ ЗАЩИТЫ «УМНОГО ДОМА»

Ликонцева Александра Андреевна
ОГБПОУ «Колледж индустрии питания, торговли и сферы услуг»
Руководитель: Лукьянова Наталья Петровна

Введение

Прогресс не стоит на месте, человечество развивается с достаточно большой скоростью и развивает всё вокруг себя. Улучшает и облегчает свой быт. Так сначала появились компьютеры и интернет, затем стали появляться вещи, которые уже подключались к интернету. Человек мог управлять ими из любой части мира, где есть Глобальная сеть. И на данный момент существуют «умные» дома, которые уже целиком работают от интернета. Меня заинтересовала эта тема тем, что для меня это что-то новое и интересное, мало кому известные технологии, хотя и широко используемые в наше время.

Моя цель узнать побольше о «умном» доме и методах его защиты, а также поделиться своими знаниями с остальными, тем самым предотвратить возможные ошибки в выборе или эксплуатации этой системы.

История создания

История Умного дома началась в прошлом веке. Первопроходцами в этой области были американцы. Собственно, понятие «Умный» дом появилось в штате Вашингтон в **Институте Интеллектуальных Зданий.** Здесь разрабатывались революционные для того времени проекты, предполагавшие возможность передачи по одному проводу различных видов информации, что позволило бы управлять разными устройствами.

Все это делалось с одной целью – **сделать более комфортной жизнь** обитателей интеллектуального жилья. Никаких других целей разработчики перед собой не ставили. УД той поры встраивался в здание на этапе его постройки и устаревал буквально на момент сдачи дома в эксплуатацию. Несовершенная проводная система не поспевала за быстрым развитием телефонных, компьютерных и других систем.

Официальной датой рождения системы УД считается 1978 г.

Система «умного» дома на тот момент представляла собой достаточно простой стандарт, посредством которого можно было выполнить всего шесть команд. Использовалась технология по большей части для управления освещением. Постепенно этого стало слишком мало. Следующий значимый этап в истории развития Умного дома приходится на 1992 год.

Современным «умным» домом можно управлять удаленно с мобильного устройства через интернет, либо с клавишных или сенсорных панелей управления. **Функционал системы чрезвычайно широк.** Он включает управление микроклиматом, безопасностью, освещением и многим другим. Оно осуществляется посредством программируемого контроллера или мини компьютера, что позволяет настраивать комплекс оборудования с учетом пожеланий и предпочтений владельца.

Специалисты характеризуют рынок систем для УД как самый быстрорастущий. На нем присутствует здоровая конкуренция между производителями из разных стран мира. Это позволяет надеяться, что в недалеком будущем интеллектуальные системы станут доступны не только состоятельным пользователям, но и всем желающим. **История Умного дома продолжается.** Поэтому вполне вероятно, что скоро появятся еще более функциональные комплексы с большими возможностями, которые сегодня нам кажутся фантастикой.

«Умный» дом — жилой автоматизированный дом современного типа, организованный для удобства проживания людей при помощи высокотехнологичных устройств. Под «умным домом» следует понимать систему, которая должна уметь распознавать конкретные ситуации, происходящие в здании, исоответствующим образом на них реагировать: одна из систем может управлять поведением других позаранее выработанным алгоритмам. Основной особенностью интеллектуального здания является объединение отдельных подсистем в единый управляемый комплекс.

Важной особенностью и свойством «Умного дома» отличающим его от других способов организации жизненного пространства является то, что это наиболее прогрессивная концепция взаимодействия человека сжилым пространством, когда человек одной командой задает желаемую обстановку, а уже автоматика всоответствии с внешними и внутренними условиями задает и отслеживает режимы работы всех инженерных систем и электроприборов.

В «умном» доме возможно с помощью одного пульта или приложения в вашем смартфоне управлять всей системой: т.е. телевизором, музыкой, освещением, видео наблюдением и т.д.

Дом сам настроит работу всех систем в соответствии спожеланием человека, временем суток, его положением в доме, погодой, внешней освещённостью и т. д. дляобеспечения комфортного состояния внутри дома.

Достоинства и недостатки системы.

Неквалифицированный труд уже не нужен: все самое сложное делают роботы, а человеку остается лишь управлять их деятельностью. Точно так же в недавнем прошлом многие обязанности в доме выполняли нанятые рабочие: охранники, дворецкие, горничные. В наши же дни этот функционал передан системе Умный дом.

Достоинства:

- ***сбережение энергии*** **-** умный дом не позволяет приборам работать «вхолостую»: обогреватель не будет включаться, когда в комнате достаточно тепло, а сплит-система не станет охлаждать улицу,
- ***безопасность*** **-** умный дом может отправить сообщение на охранный пульт, заблокировать окна и двери, проинформировать хозяев о самовозгорании и затоплении и блокировать электрические приборы, если ребенок остался дома без присмотра,
- ***оптимальный микроклимат*** **-** система ориентирована на то, чтобы в вашем доме всегда царила идеальная для здоровья атмосфера,

- ***красивый дизайн*** - не стоит бояться, что система превратит вашу квартиру в нагромождение из всевозможных приборов и проводов. Дизайн Умного дома не предполагает ничего лишнего: он незаметен в интерьере и не портит его своим видом,
- ***простота управления*** - система ориентирована на простых пользователей, которые не хотят тратить много сил и времени на то, чтобы сделать свою жизнь комфортной,
- ***развлечения*** - ваша любимая музыка может следовать за вами по всему дому, для этого вам нужен мультирум. Можно запрограммировать индивидуальный музыкальный фон для каждого этажа или помещения,
- ***система «Домашний кинотеатр»*** - это не просто набор, состоящий из колонок, сабвуфера, экрана и т.д., а целый сценарий действий. Вы выбираете функцию «Просмотр фильма»: приглушается свет, закрываются шторы, опускается экран, включается телевизор и колонки. Начинается сеанс.

Все больше набирает популярность функция «**Умный сад**», которая отвечает за автополив, дополнительное видео наблюдение и систему безопасности.

Недостатки:

Конечно, велик соблазн заявить, что **Умный дом** не имеет никаких недостатков. Однако это не так. Пожалуй, главным минусом является то, что пока система только начала внедряться на российский рынок. Поэтому редкие компании могут взять на себя монтаж системы.

Вторым минусом является относительная дороговизна Умного дома. Выше было сказано, что система со временем окупает себя за счет того, что экономит ресурсы. Однако подчас стоимость монтажа кажется чрезмерно завышенной. Однако недостаток этот вполне можно ликвидировать. Ведь большинству приспособлений, которые используются при установке системы, можно подобрать качественные, надежные аналоги отечественного производства.

Любая техника, даже самая современная периодически ломается, и если в системе управления домом выйдет из строя то-то одно, то «полететь» может приличная часть всей системы. Потому, как минимум, нужна дополнительная гарантия от установщиков и производителя.

Целесообразность. Нужно понимать, что технология разрабатывалась скорее для загородных домов, где есть автономное отопление и сложнее обеспечить безопасность. В случае с коттеджами она действительно окупается через какое-то время. Полноценная система «Умный дом» в небольшой квартире с централизованным отоплением — это скорее дорогая игрушка. Проще оборудовать квартиру хорошей сплит-системой и необходимыми датчиками, отдельной охранной системой.

Полноценная система «Умный дом» это, по сути, целый «компьютерный цех» у вас дома. Будьте готовы выделить отдельное звукоизолированное помещение под аппаратуру.

Система очень чувствительна к перепадам давления. Конечно, можно обеспечить бесперебойное питание с помощью резервного оборудования, но вы не можете застраховать оборудование от перебоев с электричеством, интернетом и т.д.

На данный момент «умный дом» — в основном, проводная технология. Поэтому установить систему можно только на стадии «черновой» отделки. Хотя на Западе уже предлагают в основном беспроводные системы.

Помните, сколько стоили первые сотовые телефоны? Еще недавно сенсорный смартфон был новым технологическим чудом, а сейчас он есть у каждого первоклассника. Новые технологии появляются очень быстро. Также быстро устаревают старые, а соответственно, падает их стоимость. Даже эта статья очень быстро устареет, потому что изменятся технологии, которым она посвящена.

Есть огромная вероятность, что самый современный на данный момент «Умный дом» через несколько лет полностью устареет. Исчезнут из продажи

нужные детали и компоненты. Скорее всего, появятся новые более дешевые решения.

Еще пару лет назад такие системы управлялись с пульта или панели и были достаточно сложными для освоения, сейчас они управляются из простого приложения в вашем смартфоне. Все больше элементов сообщаются между собой с помощью беспроводных сетей. В скором времени не будет необходимости прокладывать, в прямом смысле, километры кабелей.

Рынок систем умного дома развивается не так стремительно, как казалось еще несколько лет назад — в России встретить полностью автоматизированные дома можно довольно редко. Помимо сложности внедрения и высокой стоимости, у таких систем наблюдается еще один недостаток — умный дом можно довольно легко взломать.

Методы защиты дома

Системы умного дома или автоматизированного здания охватывают почти все области жизнедеятельности человека. Присутствуют системы автоматизации и на важных промышленных объектах: атомных станциях, нефтеперерабатывающих заводах, газопроводах. Автоматизированные системы управления (АСУ) предназначены для управления и мониторинга различных элементов автоматики. Они включают в себя управление электропитанием, сигнализацией, освещением, видеонаблюдением, системами кондиционирования, подачей тепла и т.д. АСУ обеспечивают защиту от несанкционированного вторжения на территорию здания или открытые территории благодаря системам контроля доступа.

Однако сами системы автоматизации нуждаются в информационной безопасности. Существует ряд базовых правил:

♦ разделить сеть Интернет и сети умного дома;

♦ отключить от управления автоматизированной системой жизненно важные функции здания;

♦ не устанавливать такие небезопасные функции, как, например, управление по SMS и т.д.

Безопасность стандартов автоматизации можно рассмотреть на базе нескольких важных параметров для систем автоматизации. В первую очередь, это возможность ограничения доступа к штатному контролеру, который может отправлять в сеть управляющие команды. С помощью этого контролера сервер управляет сетью автоматизации. Этот параметр называется «возможностью проведения аутентификации». Для того чтобы избежать ситуации, когда сетью будет управлять мошенник при нелегальном подключении к ней, существует ряд важных аспектов защиты сети:

♦ проверка целостности датаграмм;

♦ проверка достоверности источника;

♦ проверка принимающей стороны (конфиденциальность).

Наиболее уязвимым местом в системе умного дома, которым наверняка воспользуются злоумышленники является его подключение к сети Интернет. Большинство таких систем постоянно подключены к сети Интернет для того, чтобы Вы имели возможность следить за состоянием дома удаленно. Опытный хакер сможет получить доступ к серверу умного дома, обойдя межсетевой экран. Более того, если Вы используете мобильные приложения для управления системой, то злоумышленник может использовать уязвимости смартфона для взлома.

Более защищенные, но менее удобные цифровые дома подключаются к сети интернет на непродолжительное время, это значительно усложняет процедуру взлома, так как сервер периодически сбрасывает подключения. Наиболее безопасными считаются те версии сервера, у которых вообще отсутствует подключение к сети. Это, безусловно неудобно, однако такая система практически полностью защищена от любой атаки.

А также, многие современные системы “умный дом” во время отсутствия хозяев, умеют имитировать присутствие людей в квартире. К примеру, включают и выключают свет в разных комнатах. А некоторые системы при звонке в квартиру (или даже при прохождении мимо квартиры людей) имитируют лай злой собаки.

Кроме того, система должна правильно реагировать на возможные атаки. Атакующий может не только перехватывать данные, но и попытаться физически вмешаться в работу устройств системы, например, отключить их. В таком случае другие устройства должны заметить аномалию в виде недоступного первого гаджета.

Также существуют и так называемые взломостойкие двери, оборудованные многоуровневой системой запирания, дополнительными задвижками, а также видео домофоном.

Что еще? Если уж совсем не хватает средств на установку интеллектуальной защиты, то, уезжая в отпуск, хотя бы, попросите соседей вынимать из почтового ящика корреспонденцию и ежедневно поливать цветы. Ну и не забывайте про страхование имущества.

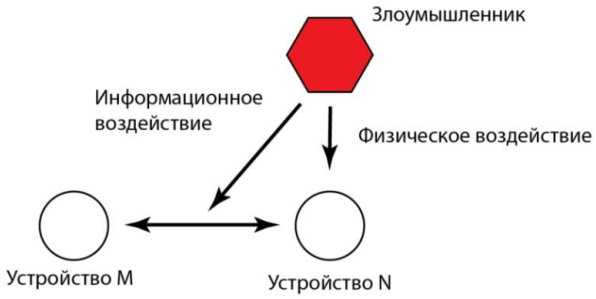


Схема воздействия на устройства системы «Умный дом». Иллюстрация из статьи «Выявление аномалий в системах автоматизации объектов охраны» авторов проекта «Безопасный умный дом».

Любая попытка атаки влияет на характеристики системы умного дома — значит их необходимо анализировать.

Чтобы обезопасить систему, необходимо в первую очередь повысить защищенность всех описанных выше слабых звеньев. Например, выбрать безопасный способ передачи данных.

Гибкость созданной безопасной умной сети позволяет объединять в ней практически любые устройства и безопасно передавать данных.

Заключение

В заключение я хочу сказать, что полноценная система «Умный дом» это однозначно не та вещь, которая делается раз и навсегда. Через 5-10 лет технологии принципиально изменятся, и старая система потеряет свою актуальность.

Если найти надежного исполнителя и качественное оборудование можно, то остановить прогресс, видимо, уже нет. С другой стороны, можно все время «смотреть на уходящий поезд» и ждать чего-то лучшего, вместо того, чтобы жить в комфортном современном доме прямо сейчас.

Не стоит стараться сделать все и сразу: система создана таким образом, что ее можно с легкостью дополнять и улучшать по мере необходимости. Начните с простого, и, войдя во вкус, вы непременно захотите делать ваш умный дом все более и более совершенным и комфортабельным!

На данный момент система «умный» дом достаточно распространена не только в жилых домах, но в предприятиях.

У системы так же, как и у любой другой существует большое количество достоинств и недостатков. Самым большим достоинством можно назвать комфорт, но, пожалуй, самым главным недостатком считается уязвимость системы. К сожалению, в настоящее время существует большое количество хакеров и взломщиков, которые пытаются не только взломать или войти, но и уничтожить всю систему. Тем не менее, благодаря прогрессу и росту человечества на любой «яд» найдётся «противоядие».

Список используемых источников:

1. http://www.ifmo.ru/ru/
2. http://blog.jammer.su/2013/01/bezopasny-li-umnie-doma-metody-zashity/
3. http://www.svoysite.info/texnologii/umnyj-dom-sovremennye-sredstva-zashhity-ot-proniknoveniya.html
4. https://dic.academic.ru/dic.nsf/ruwiki/220971
5. http://aquagroup.ru/news/7-sposobov-zashchitit-umnyy-dom-ot-vzloma.html
6. http://www.novate.ru/blogs/230317/40551/
7. https://habrahabr.ru/company/gemaltorussia/blog/281619/
8. https://habrahabr.ru/company/kaspersky/blog/311076/
9. https://mywebs.su/blog/science/29845/
10. :https://cyberleninka.ru/article/n/analiz-uyazvimostey-tehnologiy-avtomatizatsii-umnogo-doma
11. https://habrahabr.ru/company/spbifmo/blog/317454/

НЕОБХОДИМОСТЬ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ СИСТЕМ «УМНОГО ДОМА»

Кузякин А.А., Крупин М. В., Медведев В.Г., Русин А.Д.
ОГБПОУ «Томский техникум железнодорожного транспорта»
Руководитель: Извекова Эльвира Орозбековна

Аннотация: работа включает в себя рассмотрение вопросов по актуальности обеспечения мер безопасности систем «Умного дома». Рассматривается ряд систем желательных для интеграции в системы умного дома и необходимое обеспечение их безопасности. Рассмотрены различные уровни мер безопасности для различных категорий граждан.

"У́мный дом (англ. Smart House) — жилой дом современного типа, организованный для удобства проживания людей при помощи высокотехнологичных устройств. Электронные бытовые приборы в умном доме могут быть объединены в домашнюю — сеть с возможностью выхода в сети общего пользования" [1].

Стоит разделять понятия «умный дом» и «системы жизнеобеспечения». Отдельные системы обладают лишь необходимыми интерфейсами управления и контроля. Использование «Системы интеллектуального управления зданием» предполагает новый подход в организации жизнеобеспечения здания, при котором за счет комплекса программно-аппаратных средств значительно возрастает эффективность функционирования и надежность управления всех систем эксплуатации и исполнительных устройств здания.

Под термином «умный дом» обычно понимают объединение в единую систему управления зданием следующих систем:

7. Систему отопления, вентиляции и кондиционирования
8. Охранно-пожарную сигнализацию, систему контроля доступа в помещения, контроль протечек воды, утечек газа
9. Систему видеонаблюдения
10. Сети связи (в том числе телефон и локальная сеть здания)
11. Систему освещения

12. Систему электропитания здания (АВР, промышленные ИБП, дизель-генераторы)

13. Механизацию здания (открытие/закрытие ворот, шлагбаумов, электроподогрев ступеней и т. п.)

14. Управление с одного места аудио-, видеотехникой, домашним кинотеатром, мультирум

15. Телеметрия — удалённое слежение за системами

16. IP-мониторинг объекта — удалённое управление системами по сети

17. GSM-мониторинг — удалённое информирование об инцидентах в доме (квартире, офисе, объекте) и управление системами дома через телефон (в некоторых системах при этом можно получать голосовые инструкции по планируемым управляющим воздействиям, а также голосовые отчеты по результатам выполнения действий).

Само же понятие «умный дом» было сформулировано Институтом интеллектуального здания в Вашингтоне в 1970-х годах.

В нашем учебном заведении мы провели исследование среди студентов 1 и 4 курсов (возрастные группы 16-17лет и 20-21 год). В результате опроса мы выявили, что большинство студентов первого курса на сегодняшний день ознакомлены с такой технологией как «Умный дом», но незнакомы с её комплектацией. Хотели бы её иметь, но считают ее недоступной, небезопасной и подверженной сбоям. На рис.1 представлены результаты анкетирования по ряду вопросов.

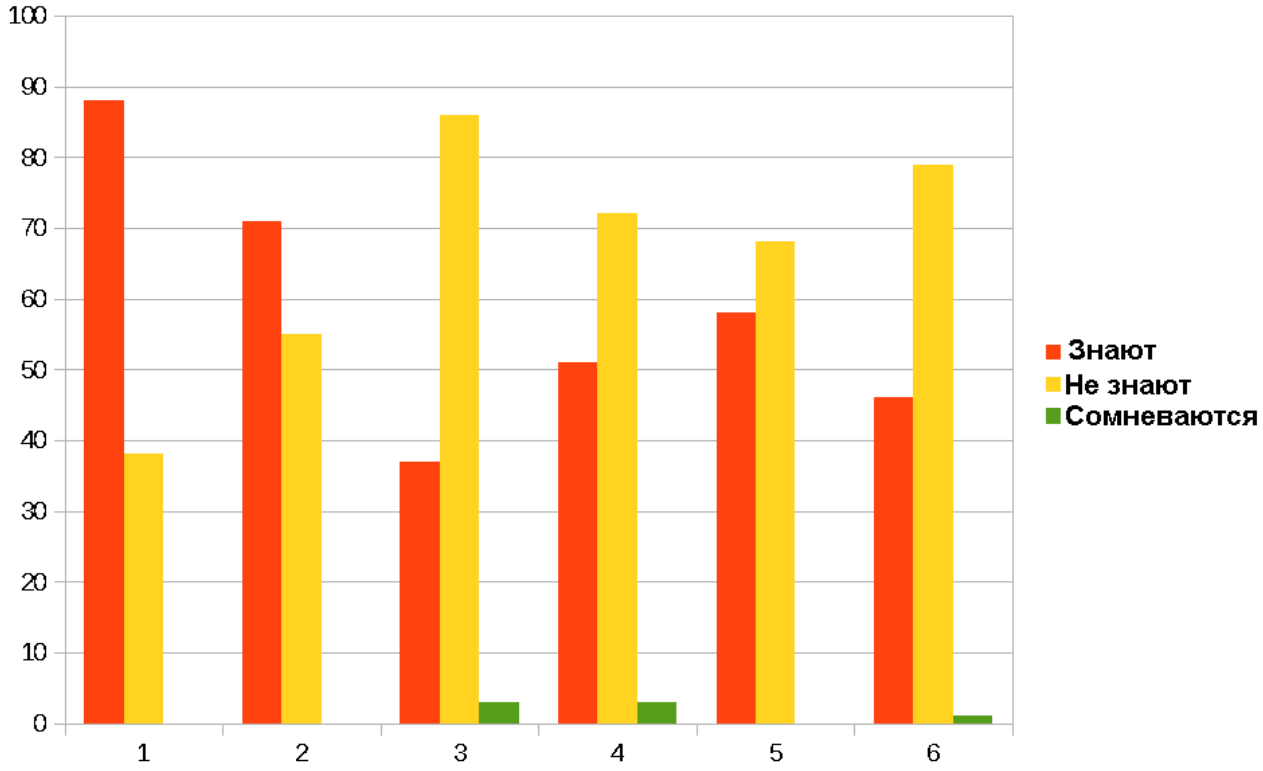


Рис. 11. Знаете ли вы что такое «Умный дом»?

2. Хотели бы вы иметь «Умный дом»?

3. Как вы считаете, насколько доступен «Умный дом» в наше время для большинства населения?

4. Что по вашему мнению входит в систему «Умный дом»?

5. Как вы считаете, является ли система «Умный дом» безопасной?

6. Как вы считаете, насколько велика вероятность сбоев в системе «Умный дом»?

В связи с выше рассмотренным опросом, мы просмотрели несколько фирм, предлагающих решения по данным системам. В зависимости от площади, количества интегрированных систем, они предлагают следующие наборы.

Квартира от 100 $м^2$ с минимальной комплектацией которая состоит из: управления освещением и подсветкой, систем управление с мобильного устройства, управление шторами, кондиционированием, датчик движения и контроля протечек воды. Данная комплектация обойдется вам в ~300 000р.

В комплектацию квартиры от 200 м^2 добавляется управление кинотеатром, управление вентиляцией и котлом отопления. Данная комплектация обойдется вам ~600 000р.

К комплектации для коттеджа площадью 500 м^2 добавляется домофон, управление бассейном, аквариумом, контроль доступа и единый пульт управления. Данная комплектация обойдется вам в ~1 500 000р.

Цены могут варьироваться в зависимости от компании в которую вы обратитесь и их комплектации. К примеру, в некоторых компаниях минимальная цена комплектации начинается от 50 000р, а максимальная может доходить до 1 500 000р. [2]

Системы «умного дома» умеют распознавать конкретные ситуации, происходящие в здании, и соответствующим образом на них реагируют. Т.е. это многофункциональные системы, обеспечивающие в доме комфорт и безопасность жителей. Модуль безопасности включает меры, направленные на предотвращение физических и информационных угроз.

К физическим угрозам можно отнести пожары, протечки, проникновение в дом без разрешения владельца, отключение электропитания и т.п. Для защиты от данных угроз в «Умном доме» присутствуют различные датчики и сигнализации, которые оповещают владельца о том, что произошло.

Современные подключенные к Интернет системы «Умный дом», как правило, соединяются через интернет с мобильным устройством или веб-браузером пользователя, позволяя таким образом контролировать их работу. И, хотя все они предназначены для обеспечения домашней безопасности, последние исследования показали, что эти устройства имеют серьезные уязвимости, из-за чего возможность осуществлять мониторинг состояния дома и его окружения может иметь не только его владелец. Основная причина недостаточной защищенности подобных устройств - это отсутствие установленных стандартов для защиты "умных" домашних систем.

Недавно компания HP опубликовала отчет исследования параметров защищенности домашних охранных систем на примере 10 самых популярных проблем безопасности для т.н. "умного подключенного дома".

Согласно статистике:

- 100% систем позволяли использовать простые пароли;
- 100% систем нуждается в механизме блокировки аккаунта, который может предотвращать автоматизированные атаки;
- 100% систем не защищены от подбора аккаунта, позволяя преступникам угадать данные аутентификации и получить доступ;
- 4 из 7 систем, которые имеют камеры видеонаблюдения, предоставляют пользователю возможность предоставить видеодоступ дополнительным пользователям, что еще больше усугубляет проблему с подбором аккаунта;
- 2 системы предоставляли возможность передачи видео вообще без аутентификации;
- Большинство камер соединяется с управляющим мобильным устройством не напрямую, а через интернет. При этом запрос, который они отправляют в интернет, не зашифрован;
- Только одна система требовала двухфакторную аутентификаци. [6]

Аналогичное исследование провела компания Synack, которая провела тестирование 16 "умных" устройств. Каждое из них (за исключением одного) было "взломано" аналитиками компании менее, чем за 20 минут.

Наиболее слабо защищенными устройствами в этом списке оказались камеры - каждая из проверенных систем имела проблемы с шифрованием данных и защищенностью паролей.

Для обеспечения безопасности данные компании предлагают принимать пользователям следующие меры:

- Использовать только временное подключение системы к интернету, что позволит снизить риск хакерских атак и минимизирует опасность появления вредоносного ПО в центральном компьютере.
- Никогда не подключаться к системе «Умный дом» из общественных мест или с чужого оборудования.
- Если приходится использовать Bluetooth и Wi-Fi, обязательно установить так называемые глушилки на тех участках, где связь выходит за пределы дома.
- Установить специальные гаджеты, препятствующие взлому и утечке информации. [4]

Гаджеты такого типа передают управление запорным механизмом мобильным устройствам. При его приближении устройство снимает блокировку двери. Можно осуществлять управление механизмом и дистанционно. Есть модели, которые открываются голосовой командой, и это самая уязвимая разновидность.

Взлом умного замка возможен, если злоумышленник получил к нему физический доступ. Если это произошло, он может нажатием клавиши авторизовать свой смартфон, после чего без проблем открыть дверь в любой подходящий момент. Во избежание этого следует обязательно деактивировать функцию подключения других мобильных устройств в настройках умного замка.

Список используемых источников:

1. https://domashke.net/referati/referaty-po-informatike/referat-sistemy-umnyj-dom

2. http://mimismart.ru/smart-home/bezopasnost/

3. Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О.В. Прохорова. — Электрон. текстовые данные. — Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 113 с. — 978-5-9585-0603-3. — Режим доступа: http://www.iprbookshop.ru/43183.html

4. http://tech-house.su/kak-zashhitit-umnyj-dom-ot-vzloma/

5. Информационная культура личности [Электронный ресурс] : учебно-методический комплекс по направлению подготовки 09.03.03 (230700.62) «Прикладная информатика», профиль «Информационная сфера», квалификация (степень) выпускника «бакалавр» / . — Электрон. текстовые данные. — Кемерово: Кемеровский государственный институт культуры, 2014. — 132 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/29663.html

6. https://www.ferra.ru/ru/digihome/review/SmartHome-CyberSecurity/ - Сергей Головин

«УМНЫЕ» СЕТИ ДЛЯ ВЫСОКИХ ТЕХНОЛОГИЙ

Караманец Б.Р., Байдебура М.А.
Республиканский многопрофильный лицей-интернат при ДонНУ, г. Донецк, ДНР
Руководитель: Гридина Валерия Валериевна

Актуальность исследования. В последние годы в России наблюдается растущий интерес к бурно развивающемуся во всем мире направлению преобразования электроэнергетики на базе новой концепции, получившей название «умные» сети (Smart Grid). Smart Grid является концепцией инновационного преобразования электроэнергетики, пересмотр ряда существующих базовых принципов модернизации отрасли и вытекающие отсюда масштабы и характер задач обусловливают повышенное внимание к данной концепции [1].

Технология «умных» сетей (Smart Grid) является наиболее эффективным решением проблемы увеличения коэффициента полезного действия (КПД) и снижения затрат на транспортировку электроэнергии.

В перспективе использование «умных» сетей для распределения и транспортировки электроэнергии должно способствовать решению мировых проблем в энергетике, экономике и экологии.

Целью исследования является определение преимуществ и недостатков «умных» сетей (Smart Grid), а также проблем, возникающих при ее использовании.

«Умные сети» являются приоритетным направлением в энергетике на сегодняшний день. Впервые данный термин был употреблен Массудом Амином и Брюсом Волленбергом в публикации «К интеллектуальной сети» в 1998 г. [2].

Smart Grid — это автоматизированная система, которая самостоятельно отслеживает и распределяет потоки электричества для достижения максимальной эффективности использования энергии. В мире, где защита природных ресурсов стала одним из главных приоритетов, очень важно найти дешевые и эффективные пути снижения их использования [3].

В мировой практике для определения «умной» сети используются ее атрибуты или признаки (табл. 1) [2].

Таблица 1

Признаки определения «умной» сети

США	Европейский союз	Россия
способность к самовосстановлению после сбоев в подаче электроэнергии.	гибкость-сеть должна подстраиваться под нужды потребителей электроэнергии.	насыщенность сети активными элементами, позволяющими изменять топологические параметры сети.
возможность активного участия в работе сет потребителей	доступность-сеть должна быть доступна для новых пользователей, причем в качестве новых подключений к глобальной сети могут выступать пользовательские генерирующие источники.	большое количество датчиков, измеряющих текущие режимные параметры для оценки состояния сети в различных режимах работы энергосистемы.
устойчивость сети к физическому и кибернетическому вмешательству злоумышленников	надежность - сеть должна гарантировать защищенность и качество поставки электроэнергии в соответствии с требованиями цифрового века.	система сбора и обработки данных (программно-аппаратные комплексы), а также средства управления активными элементами сети и электроустановками потребителей.
обеспечение требуемого качества передаваемой электроэнергии	экономичность - наибольшую ценность должны представлять инновационные технологии в построении Smart Grid совместно с эффективным управлением и регулированием функционирования сети.	наличие необходимых исполнительных органов и механизмов, позволяющих в режиме реального времени изменять топологические параметры сети, а также взаимодействовать со смежными энергетическими объектами.
обеспечение синхронной работы источников генерации и узлов хранения электроэнергии	безопасность - не допущение ситуаций в электроэнергетике, опасных для людей и окружающей среды.	средства автоматической оценки текущей ситуации и построения прогнозов работы сети.

появление новых высокотехнологичных продуктов и рынков.		высокое быстродействие управляющей системы и информационного обмена

В условиях современной российской экономики предприятию для получения большей прибыли необходимо снизить потребляемую энергию, именно стоимость затрат на электроэнергию является определяющим фактором конкурентоспособности предприятия, при условии невозможности проведения модернизации оборудования. Появление новых технологий, которые способны на какую-то долю обеспечивать себя электроэнергией привело к созданию «умных» сетей. Опыты в этой области начали проводить ученые Европы и США уже с 1970 года.

Основными преимуществами внедрения технологии «умных» сетей (Smart Grid) являются:

1. Повышение управляемости и наблюдаемости сети.

2. Снижение потерь электроэнергии.

3. Управление отключениями в режиме реального времени.

4. Повышение надежности сети

5. Сокращение ущерба от аварий и сроков восстановления работоспособности.

6. Построение прозрачной системы учета и биллинга на основе данных о фактически переданной и потребленной энергии.

7. Оптимизация планирования и снижение затрат на ТОиР

8. Повышение уровня сервиса для потребителей

9. Включение потребителей в процессы управления энергией и энергосбережения

10. Интеграция в общую энергосистему возобновляемых источников энергии и систем энергонакопления.

Несмотря на большое количество преимуществ внедрения технологии «умных» сетей (Smart Grid) существует и ряд недостатков, таких как угроза

частной жизни, риск хакерских атак, коррупция, усложнение расчета платы из-за динамического ценообразования.

Инициативы по развертыванию «умных» сетей (Smart Grid) в Европе сталкиваются с рядом проблем ставших уже традиционными, такими как неопределенность в финансировании проектов, беспокойство в части защиты личных данных потребителей, пробелы в обеспечении регулирования отрасли и стандартизации применяемых технологий и, наконец, отсутствие мотивации у конечных потребителей. Тем не менее, рынок «умных» сетей (Smart Grid) сигнализирует участникам об уверенном росте [4].

Внедрению «умных» сетей в России препятствуют многие факторы, такие как финансовые факторы, непонимание работы сети, недостаток обученных специалистов в данной сфере.

Основными проблемами, которые препятствуют распространению технологии Smart Grid в России и в мире, являются [5]:

1. Значительное количество потребителей, предъявляющих разные требования к качеству электрической энергии.

2. Отсутствие надежных накопителей энергии.

3. Значительные финансовые вложения в процессе внедрения системы «умных» сетей (Smart Grid) и ее последующего обслуживания.

4. Отсутствие стандартов и нормативов.

5. Отсутствие мотивации у генерирующих компаний, так как их прибыль напрямую зависит от объемов проданного электричества, а при введении новой технологии доходы могут значительно снизиться.

Несмотря на существующие проблемы и недостатки внедрения, «умные» сети способны обеспечить общественное развитие, прорывное повышение потребительских свойств и эффективности использования энергии с учетом всех факторов развития электроэнергетики в будущем.

Вывод. Таким образом, на основе проведенного исследования можно сделать вывод о том, что «умные» сети (Smart Grid) противостоят физическим и информационным негативным воздействиям без тотальных отключений или

высоких затрат на восстановительные работы, при этом имеют максимально быстрое восстановление.

Список используемых источников:

1. Кобец Б.Б. Инновационное развитие электроэнергетики на базе концепции Smart Grid [Электронный ресурс] / Б. Б. Кобец, И. О. Волкова — М.: ИАЦ Энергия, 2010. — 208 с. Режим доступа: URL: https://www.hse.ru/data/2013/01/23/1306487070/SmartGrid_monografia.pdf (дата обращения 19.11.2017)

2. Smart Grid или умные сети электроснабжения [Электронный ресурс] Режим доступа: URL: http://www.fortnightly.com/fortnightly/2003/11/ technology-corridor (дата обращения 19.11.2017 г.)

3. Решения Моха для построения интеллектуальных энергосистем [Электронный ресурс] Режим доступа: URL: https://www.nnz-ipc.ru/files/publ/1872274/files/assets/basic-html/page3.html (дата обращения 19.11.2017 г.)

4. Ледин С.С. Обзор инициатив в области Smart Grid в мире и России [Электронный ресурс] / С.С. Ледин // Автоматизация в промышленности, 2013. – № 1 Режим доступа: URL: http://www.sicon.ru/about/articles/?base=&news=30 (дата обращения 22.11.2017г.)

5. Мировой и российский рынок технологий SMART GRID [Электронный ресурс]. Режим доступа: URL: http://www.cleandex.ru/articles/2010/04/13/smart_grid_market (дата обращения 19.11.2017 г.)

СЕКЦИЯ 3. «ЗАЩИТА ПРАВ И ИНТЕРЕСОВ ГРАЖДАН В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ»

ИНФОРМАЦИОННАЯ КУЛЬТУРА КАК РЕСУРС ОБЕСПЕЧЕИЯ БЕЗОПАСНОСТИ ЛИЧНОСТИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Сухова Алина Федоровна
ОГБПОУ «Томский политехнический техникум»
Руководитель: Рязанова Галина Михайловна

В контексте информационной культуры рассматриваются отдельные актуальные проблемы обеспечения безопасности личности в формирующемся информационном обществе. В данной работе представлены императивы личностного освоения информационной культуры, среди которых особая роль отведена современному информационному мировоззрению и воздействию на него средств массовой информации и коммуникации, в том числе интернета.

На каждом историческом этапе цивилизационного развития человеку приходилось адаптироваться к различным природным, а затем и искусственно созданным им самим условиям существования. Реалии современного информационного общества в качестве категорического императива поставили перед ним проблему адаптации к информационной среде как важнейшей составной части окружающей среды обитания. Сегодня ситуация радикально изменилась: информация сама превратилась в важнейший вид деятельности, а средства информационного взаимодействия обновляются с огромной скоростью, что выдвигает весьма жесткие требования к информационной культуре личности и общества в целом.

В формирующемся информационном обществе информация и знания создают невиданные ранее возможности развития социума, а интеллект и знания становятся главными доминантами общего развития цивилизации. Однако преимущества информационного общества нельзя воспринимать как абсолютные, в них множество противоречий и даже опасных тенденций, как:

-усиление манипулирования общественным сознанием

-информационное излишество, или "синдром информационной усталости", накладывающий отпечаток на принятие управленческих решений:
-уход в "виртуальный мир", провоцирующий резкое сокращение "живых" личностных коммуникаций
-пагубное воздействие биопатогенных полей, связанных с работой электронных устройств
-информационное неравенство людей и общества

Императивы личностного освоения информационной культуры в современном обществе - это, прежде всего:
-*теоретические знания*, касающиеся сущности, содержания особенностей и закономерностей её функционирования в обществах с различными уровнями информатизации
-сформированное *информационное мировоззрение,* позволяющее выстраивать собственную стратегию информационной деятельности.
-"*информационная этика"* общения в социальных компьютерных сетях, нравственный информационно-коммуникационный разговор
-информационная грамотность, включающая в себя: умение определять и формулировать свои *информационные потребности и запросы,* оперативно проводить эффективный самостоятельный *поиск информации,* используя традиционные и нетрадиционные электронные поисковые системы, знания *современных информационных технологий и владение ими*, умение их применять в профессиональной и повседневной деятельности.

Интернет приносит в нашу жизнь много удобств, и много пользы. В наше время уже совсем не обязательно иметь огромную домашнюю библиотеку, так как любую нужную книгу уже можно найти в интернете. Кроме этого в сети есть много интересных рецептов по приготовлению блюд с пошаговой инструкцией, то есть с его помощью можно научиться, отлично готовить. И теперь совсем не обязательно долго искать в кулинарной книге определенное блюдо, достаточно написать название в интернете и сразу же найдется рецепт. Разве это не польза? И это еще минимум того что дает интернет.

Интернет облегчает жизнь многим людям. В работе человека он очень практичный и удобный, если раньше данная работа выполнялась в течение двух, а то и трех дней, то сегодня с помощью мировой сети можно сделать всю работу всего за час.

Многие люди инвалиды могут теперь только с помощью компьютера и наличии интернета выполнять работу дома и тем самым зарабатывать себе на жизнь.

Интернет так же выполняет познавательную роль, вы можете путешествовать по всему миру, не отходя от своего компьютера. Перед вами открывается весь земной шар со своими райскими уголками. Теперь не нужно тратить кучу денег и покупать различные энциклопедии, достаточно только открыть поисковую систему и прописать интересующий вас вопрос.

В последние время у любой организации или отдельного лица имеется очень большое количество обобщенной информации, которая хранится в интернете или на компьютерах. Такое большое количество информации стало причиной того, что очень часто происходит ее утечка, но никто не хотел бы, чтобы засекреченная и конфиденциальная информация о чем-либо попала к посторонним лицам, собственно для этого и нужно применять меры предосторожности по обеспечению информационной безопасности.

Информационная безопасность — это комплекс мер, среди которых нельзя выделить более или менее важные. И иначе ее воспринимать нельзя. Здесь важно все! Меры защиты нужно соблюдать во всех точках сети, при работе любых субъектов с вашей информацией (под субъектом в данном случае понимается пользователь системы, процесс, компьютер или программное обеспечение для обработки информации). Каждый информационный ресурс, будь то компьютер пользователя, сервер организации или сетевое оборудование, должен быть защищен от всевозможных угроз. Защищены должны быть файловые системы, сеть и пр.

Использование Интернета является безопасным, если выполняются ТРИ ОСНОВНЫХ ПРАВИЛА:

1. Регулярно обновляйте операционную систему, используйте антивирусную программу, применяйте брандмауэр, создавайте резервные копии важных файлов, будьте осторожны при загрузке содержимого.
2. Никогда не разглашайте в Интернете личную информацию, за исключением людей, которым вы доверяете. При запросе предоставления личной информации на веб-сайте всегда просматривайте разделы «Условия использования» или «Политика защиты конфиденциальной информации», чтобы убедиться в предоставлении оператором веб-сайта сведений о целях использования получаемой информации и ее передаче другим лицам. Всегда удостоверяйтесь в том, что вам известно, кому предоставляется информация, и вы понимаете, в каких целях она будет использоваться.
3. При работе в Интернете будь вежлив с другими пользователями Сети. Имена друзей, знакомых, их фотографии и другая личная информация не может публиковаться на веб-сайте без их согласия или согласия их родителей. Разрешается копирование материала из Интернета для личного использования, но присвоение авторства этого материала запрещено. Передача и использование незаконных материалов (например, пиратские копии фильмов или музыкальных произведений, программное обеспечение с надорванными защитными кодами и т.д.) является противозаконным.

Проверка сайта на мошенничество – все возможные способы

Проверка сайта на мошенничество – это комплекс действий, которые необходимы для выявления неправомерной активности со стороны веб-сайта.

Ежедневно в интернете создается около 1 миллиона сайтов, которые зарегистрированы по всему миру. 15% от этой цифры – ненадёжные источники, которые принято называть фишинговыми или мошенническими сайтами.

Наверняка, каждый человек хотя бы раз видел в интернете рекламу о том, как за минимальное время заработать много денег или найти работу через посредника.

Многие такие рекламки ведут на ненадёжные сайты, где у юзеров требуют перевести деньги. Затем сайт просто закрывается или меняется его домен, чтобы пользователь не смог пожаловаться.

Признаки ненадёжных ресурсов

Определить уровень доверия к конкретному сайту может любой пользователь. Для этого нужно знать лишь те параметры, на основе которых происходит оценка опасности ресурса. Рассмотрим некоторые из них:

- *Отсутствие репутации.* Нашли новый интернет-магазин с привлекательными ценами или выгодные предложения с возможностью предоплаты? Если вы используете сайт впервые, ни в коем случае не нужно отправлять деньги без проверки веб-страницы. Первое, что вы можете сделать – поискать информацию о сайте в поисковых системах. Отсутствие отзывов пользователей или упоминаний в запросах – это первый признак мошенников;
- *Легитимность*. Даже если по вашему запросу сайт оказался в топе поисковой выдачи, это еще не говорит о его надёжности. Сервисы для проверки веб-адресов показывают, что фишинговые источники часто являются лидерами выдачи. Такого результата они достигают с помощью накрутки запросов или рекламы;
- *Ошибки в контенте*. Владельцам фишинговых сайтов приходиться очень часто переносить их с одного домена на другой или создавать новые, так как они быстро блокируются. Все это сказывается на оформлении и контенте. Если вы нашли много очевидных ошибок в словах, лишние знаки – это один из признаков опасности;
- *Адреса страниц*. На большинстве фишинговых сайтов все его странички имеют один и тот же веб-идентификатор. Попробуйте перейти на другие вкладки ресурса и посмотрите, меняется ли текст в адресно строке браузера;

- *Оригинальность.* Если вы ищите ресурс конкретной организации или магазина, не переходите по внешним ссылкам из социальных сетей или электронных писем. Посмотрите название компании и введите его в поисковой системе в форме запроса «сайт «название организации»»;
- *Срок работы ресурса.* Дата регистрации страницы – это один из показателей её надежности. Если возраст сайта 2-3 дня, а он уже имеет внушительный счетчик платежей, скорее всего, он фишинговый. Проверить время работы ресурса можно с помощью специальных сервисов, которые описаны ниже в статье.

Проверка надежности с помощью онлайн сервисов

Стоит помнить, что каждый день создается масса фишинговых сайтов, поэтому следует проверять подозрительные источники не только с помощью ранее составленных списков, но и воспользоваться онлайн сервисами для анализа, такими как:

1. **AdvisorWebmoney-** рекомендуется применять этот сканер для проверки онлайн-обменщиков или других сайтов, на которых можно совершить оплату.
2. **Mirzam-**проводиться анализ IP адреса, обнаружение даты регистрации, использование защищённых соединений.
3. **Сервис «Доверие в сети»-**это еще один полезный источник для выявления опасных сайтов. Чтобы определить репутацию странички, скопируйте её адрес в текстовое поле нажмите на клавишу «Проверка». Итог анализа будет содержать уровень траста, название домена, процент риска, возраст домена и другие показатели.
4. **AvastOnlineSecurity (расширение для браузера)-** устанавливается утилита в качестве расширения для вашего браузера. Переходя на неизвестный сайт, вы сразу увидите всплывающее окно, которое покажет уровень безопасности ресурса.

Семь советов по защите от ненадёжных сайтов

Чтобы не попасться на уловки фишинговых сайтов и мошенников, следует придерживаться таких правил:

- Старайтесь не оставлять свой номер телефона и электронную почту на других сайтах. Советуем не подписываться на рассылки неизвестных ресурсов;
- Оплачивайте покупки только на проверенных сайтах, используя защищённое соединение. Желательно, совершать транзакции с помощью официального онлайн-банкинга;
- Используйте антивирусные программы. Антивирус способен анализировать подозрительные сайты и их запросы, блокируя их;
- Работайте с Open DNS. Это утилита для фильтрации фишинговых сайтов и блокировки рекламы. Работая в фоновом режиме, она мониторит действия пользователя и исправляет опечатки в названиях сайтов, предотвращая переход на сторонние ресурсы. Существует, платная и бесплатная версия программы;
- Создавайте уникальные пароли для каждого сайта. Многие юзеры используют один и тот же пароль на всех сайтах. Это упрощает работу хакерам;
- Мониторьте новые сайты с помощью сервисов для проверки надёжности;
- Не соединяйтесь с открытыми сетями Wi-Fi.

Вывод: формирование информационной культуры личности является на современном этапе одним из приоритетов государственной культурной политики и важнейшей задачей педагогического процесса. В акцент информационного общества акцент делался на всеобщую доступность информации, обеспечиваемую через внедрение новых информационно-коммуникационных технологий. Однако вскоре стало ясно, что обилие, разнообразие поступающей информации, а также оперативность её доставки ещё не является гарантией осведомленности и компетенции личности общества в целом, а также это не означает, что способы получения этой информации будут безопасны. В данной работе, я рассмотрела императивы личностного освоения информационной культуры, провела анализ признаков надежности различных ресурсов. В современном обществе каждый день создаются масса фишинговых сайтов,

с помощью которых мошенники обманывают через отправления смс со ссылкой на какой-то сайт, либо неосведомленных людей, либо студентов, детей. Поэтому мною были исследованы такие онлайн сервисы, которые могут проверить надежность подозрительных источников.

Список используемых источников:

1. Учебно-методическое пособие, г.Москва: Либерия-Бибинформ : «Информационная культура личности», Дулатова А.Н., Зиновьева Н.Б., 2007г., ст.70
2. Основные понятия и анализ угроз информационной безопасности «Лаборатория Сетевой Безопасности» http://ypn.ru/102/introduction-to-information-protection-and- information-security/
3. Чурашева О.Л. Библиометрический анализ публикаций по проблеме формирования информационной культуры личности//Библиосфера.2014. №3. С.69-73 https://cyberleninka.ru/article/n/informatsionnaya-kultura-i- informatsionnaya-bezopasnost-lichnosti
4. Кириленко А.В. Основы информационной культуры, учебное пособие, г.Санкт-Петербург 2008г.
5. Проверка сайтов на мошенничество «Компьютерная помощь» https://pomogaemkompu.temaretik.com/1162965306737166666/proverka-sajta-na-moshennichestvo---vse-vozmozhnye-sposoby/

«ЗАЩИТА ПРАВ И ИНТЕРЕСОВ ГРАЖДАН В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ»

Михайлов Юрий Андреевич

ОГБПОУ «Техникум информационных технологий»

Руководитель: Грушевский Юрий Викторович

Введение

В данном докладе дается определение базовых понятий предметной области, а также отражается общая интенция, связывающая следующие аспекты информационной безопасности: историко-хронологические этапы развития информационной безопасности, средства информационного воздействия на общественное сознание, правовые аспекты обеспечения информационной безопасности, а также право граждан на информацию. Рассматривается проблематика конфликта в подходах к информационной безопасности в современном мире. Сопоставляются точки зрения конфиденциального подхода и случаев, когда ими приходится пренебрегать в угоду общественных интересов. Рассказывается о преимуществе открытости информации, сопоставляя идеи авторского права и возможности получать информацию в порядке свободного доступа. Затрагиваются философские аспекты сути времени, в котором мы живем, и то, как они влияют на информационное поле.

Определения[1]

Информационная безопасность – это состояние информационной среды, которое достигается (организуется) необходимыми мерами. Критериями этих мер являются: конфиденциальность, доступность, целостность, достоверность, а также защита законных прав личности и общества в информационной среде.

Конфиденциальность – это требование к информации определенного рода, которое заключается в неразглашении без дополнительного согласия

того, к кому эта информация имеет отношение, с другой стороны в ряде случаев основанием для получения ее может послужить законное требование со стороны правоохранительных органов.

Конфиденциальной информацией являются следующие сведения:

- Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаев.
- Сведения, составляющие тайну следствия, а также сведения о защищаемых лицах и мерах государственной защиты.
- Служебные сведения – которые связаны с понятием гос. тайны.
- Профессиональная деятельность – врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и других сообщений.
- Сведения, связанные с коммерческой деятельностью – коммерческая тайна.
- Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

  Также стоит отметить, что пользователь может сам наделить любую информацию таким статусом.

Целостность – неизменность информации в процессе ее передачи и хранения.

Доступность – возможность получения доступа и использование информации по требованию уполномоченных лиц.

Рассмотрев вводные понятия, мы можем изучить исторические аспекты развития информационной безопасности.

Исторические аспекты возникновения и развития информационной безопасности[2].

- I этап — до 1816 года — Внетехнологический период. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих жизненное значение для человека лично или сообщества, к которому он принадлежал.
- II этап — начиная с 1816 года — связан с использованием создаваемых технических средств электро- и радиосвязи. Для обеспечения помехозащищенности радиосвязи необходимо было использовать старый опыт защиты информации и дополнять его новыми техническими требованиями.
- III этап — начиная с 1935 года — связан с появлением радиолокационных и гидроакустических средств. Основными мерами безопасности стали технические меры, повышающие защищенность радиолокационных средств от воздействия на их приемные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами.
- IV этап — начиная с 1946 года — связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин. Задачи информационной безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию.
- V этап — начиная с 1965 года — обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты технологических средств, объединённых в локальную сеть путём администрирования и управления доступом сетевых ресурсов.
- VI этап — начиная с 1973 года — связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Для обеспечения информационной безопасности в компьютерных системах с беспроводными сетями передачи данных потребовалась разработка

новых критериев безопасности. Образовались сообщества людей — гиков и хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности — важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право — новая отрасль международной правовой системы.

- VII этап — начиная с 1985 года — связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

Средства информационного воздействия на общественное сознание.

Стоит отметить, что уже в прошлом столетии способы отражения явлений в мировой и общественной жизни были кардинально пересмотрены, реализм как способ выражения классической картины мира, приказал долго жить. Исчез вместе с его устаревшими понятиями, также как устарели формы монархии, которые перестали удовлетворять нуждам современного человека и его общества. Аграрный труд стал вытесняться мануфактурами и фабриками, технический прогресс неукротимо шагал своими большими шагами, и тот кризис, который образовался в результате неудовлетворенного коллективного бессознательного масс и изжившего себя недальновидного на тот момент миропорядка породил революцию в художественном мире и мире искусств, ознаменовав пришествие авангарда, позже революция пришла и в социальное пространство. Модернисты занимались тем, что искали новые способы выражения в искусстве, затем на смену их форм пришел «век» постмодернизма, который в своем роде являлся эклектикой жанров, всевозможным смешением их.

Этот способ отображения до сих пор остается актуальным и отражает суть времени, в котором мы живем. Может быть не совсем очевидно, но если обратить внимание на СМИ, то можно почувствовать, что мы живем в мире, информационное пространство которого соткано из мифов. Более того, их структура не такая простая, какой может оказаться на первый взгляд. За одним мифом скрывается другой, за вторым третий, современность также ловко переворачивает идеи, которые не угодны определенным группам, правительственным или высшим кругам, протестные идеи переворачиваются, и заменяются симулякрами, например, идея о борьбе за права женщин – теперь популяризирована настолько, что за ее счет пиарятся крупные политические деятели, такие как Хилари Клинтон в своей агитационной программе. При этом, она является представителем элиты, которой нет никакого дела до защиты прав угнетенных групп населения. Многие протестные идеи, которые были созданы, чтобы освобождать, превращаются в тренд, и теряют свою силу в том проявлении, в котором существуют сейчас. Сама суть этого времени подразумевает, что больше нет ни хорошего, ни плохого. СМИ также умело использует эти образы, чтобы призывать людей к чему либо. Например, на войну, романтизируя ее, используя старые образы защитника рода или же семьи. Но стоит отметить, что как таковой, этот образ мертв в нашем современном веке, ты идешь воевать не за мир в твоем доме, а совершаешь убийства в мясорубке, в которой и сам толком ничего осознать не можешь, как у классика: «Все смешалось, люди, кони». Цель СМИ - вторить какой либо популистской политической линии, даже после того протеста, которым горел весь мир, осознав бессмысленность первой мировой войны, в ходе которой этому миру открылась вся абсурдность этого занятия, такая как: война за лидеров, которым плевать на жизни людей. Не наша война. Примеров можно приводить множество, но одно можно сказать точно: вещи не являются такими, какими они кажутся, без возможности детального их рассмотрения. Мы живем в век корпораций, тотального контроля и слежки, узкая группа людей пытается формировать наши

вкусы, взгляды на жизнь, философию. И все бы было хорошо при данном раскладе, если бы не завуалированность истинных целей тех структур, что довлеют над нами. Непрозрачность их истинной этики и преследуемых целей. В виду этого, информационная культура должна иметь возможность развиваться в различных направлениях. Исходя из этого, мы должны учитывать, что важным в информационном поле является этический и культурный аспект, важным является становление независимой информационной культуры, которая бы уравновешивала систему коммерчески-закрытой информации, такой культурой является хакерство, или же просто распространение идей о свободе информации в открытом мире, который будет иметь возможность развиваться в различных направлениях и взращивать независимые взгляды на этические аспекты информационного пространства.

Организационно-правовые аспекты обеспечения безопасности информационно-телекоммуникационных сетях.

В общем случае они могут быть сгруппированы в следующие категории[3]:

1. Федеральные правовые документы, которые включают в себя кодексы и законы, указы и распоряжения Президента РФ, а также постановления Правительства РФ;
2. Отраслевые нормативные документы, включающие в себя российские и *международные стандарты*, а также специальные требования Федеральной службы по техническому и экспортному контролю (ФСТЭК) и ФСБ, касающиеся вопросов *защиты информации*;
3. Локальные организационно-распорядительные документы, которые действуют в рамках отдельно взятой организации, например, должностные инструкции, приказы, распоряжения и другие документы, касающиеся вопросов *информационной безопасности*.

Право граждан на информацию.

Это совокупность правовых понятий, в которые входят права на свободу мыслей, свободу слова, свободу печати. Свобода искать, получать и распространять информацию, является одним из важнейших политических и личных прав человека и включена во Всеобщую декларацию прав человека.

Вместе с тем, свобода информации может быть ограничена, как для соблюдения других прав личности (тайна связи, защита от вмешательства в личную и семейную жизнь), так и для защиты интересов общества (ограничения в период чрезвычайного или военного положения).

Вывод

Информационная безопасность с учетом новых условий технологического развития, а также современного информационного поля принимает новые формы, стоит учитывать то, что сопутствует этому понятию, например, такие вещи, как дух времени. Актуальным является проблематика конфликта, между такими позициями как конфиденциальность или же необходимость вмешательства в личную жизнь человека под предлогами защиты общественных интересов или же интересов государства. Актуальным является поиск

уравновешенной позиции по данному вопросу. Не менее важной на сегодняшний день остается вопрос во взглядах на доступность информации, стоит сказать об авторских правах, например, авторские права могут быть неуместны в том случае, когда для исследовательских работ нам необходима современная научная литература. Здесь мы можем обратить внимание на противостояние культуры хакеров данному явлению, на понятие о свободном информационном пространстве, которое определяет доступность научной и культурной среды для всех, а не только при наличии возможности заплатить за доступ к данной информации. Это и есть противостояние капиталистического подхода и социалистического в современной интерпретации. Мне симпатичен взгляд, когда вне зависимости от социального статуса, заинтересованный может заниматься наукой или же получать культурное образование, и деньги в этом вопросе не будут играть какой-либо роли. Затрагивая эту тему, я хочу привести в пример пиратский портал Sci-Hub, сутью которого является предоставление бесплатного доступа к научным статьям, доступ к которым на других ресурсах требует внесения определенной платы. Этот сайт был организован Александрой Элбакян[4], девушкой-хакером из Казахстана, которая стала человеком года в 2016 году по версии журнала Nature, одновременно став и самым влиятельным человеком в области науки за этот же год.

Список используемых источников:

1. Определения составлены и заимствованы на основе словарей ресурса https://dic.academic.ru а именно: «Словарь-справочник терминов нормативно-технической документации».
2. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2000. — 428 с — ISBN 5- 93598-030-4. (хронология развития и этапы информационной безопасности)
3. Сайт: http://www.intuit.ru Лекция: «Организационно-правовые аспекты защиты информации»

4. Известная статья: Создательница «пиратского» портала научной литературы стала человеком года по версии журнала Nature. Источник: roskomsvoboda.org

ВЕБ – ПОРТФОЛИО КАК ОСНОВА ЗАЩИТЫ ПРАВ И ИНТЕРЕСОВ СТУДЕНТА

Трофимов Михаил Олегович
ОГПОУ «Томский базовый медицинский колледж»
Руководитель: Смоляр Овсей Борисович

Исторически портфолио возникло как сборник, хранилище документов, достижений студента, в котором информация хранится в бумажной форме. Требуется пополнять, видоизменять его новым содержимым по мере необходимости в течение всего периода обучения. Например, добавив сертификат участника конференции, призера олимпиады и т.д. В нужный момент, студент предъявляет его соответствующим органам, структурам.

Необходимость портфолио в студенческой жизни:

- п*ерспективная работа или подработка;*
- *участие в олимпиаде, конференции;*
- *участие в волонтерском движении, художественной самодеятельности;*
- *достижения в спорте;*
- л*ичные цели;*
- *семейная жизнь* и др.

Каким образом подобное решается в образовательных учреждениях? С 2011 года практически во всех общеобразовательных учреждениях оформление портфолио ученика является обязательным. Составлять его необходимо уже в начальной школе [1]. На уровне колледжей, техникумов отсутствует стандартный подход. Каждое образовательное учреждение, школьник, студент, выходят из положения как могут, по-разному:

- составляют портфолио на бумаге;
- используют самодельные программы;
- создают свои или используют существующие сайты;
- применяют для создания и хранения портфолио систему дистанционного образования (типа Moodle) и др.

Однако, как только учащийся перевелся в иное образовательное учреждение, либо закончил обучение доступ к своему портфолио становится затруднительным. Да и вышеназванные подходы не обеспечивают удовлетворения всех требований, предъявляемых к ВЕБ-портфолио, ограничивают права и интересы обучающихся.

С появлением и бурным развитием информационно-телекоммуникационные технологий, появилась возможность портфолио (ВЕБ-портфолио) размещать на портале, сайте. Теперь его можно создать, просматривать, редактировать содержимое, дополнять информацией любого вида и в любое время: текстовой, графической, видео, звуковой. Отныне возможно отражать в портфолио динамику студенческой жизни каждым.

С точки зрения ФЗ о персональных данных – « … целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных. В том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну».

В нашем колледже используем социальную отечественную сеть 4portfolio.ru, которая предназначена для конструирования портфолио, сбора и хранения, полного отчета об успехах и достижениях, позволяет общаться, обучаться дистанционно [2]. К тому же имеется возможность формирования резюме, ведение записных книжек и блогов. Дополнительно реализована возможность общаться со своими друзьями, создавать и вступать в сообщества и все это бесплатно. Студенты во время занятия осваивают работу в социальной сети для создания своего ВЕБ-портфолио. За период обучения частенько возникает потребность в предоставления доступа к части портфолио друзьям, работникам администрации учебного заведения и т.д. Как же подобное решается в ВЕБ-портфолио? Ответ очевиден, достаточно студенту ввести электронный адрес того лица, кому он желает предоставить доступ, определить статус и временной период доступа, указать раздел(ы), к которым предоставляется доступ.

Отсюда вытекают требования, ВЕБ-портфолио должно быть доступно только самому студенту в течение 24 часов в сутки независимо от места

учебы, его географического нахождения. Причем, каждый обучающийся должен иметь возможность предоставлять доступ к части персональным данным, тем, структурам, физическим лицам, потенциальным работодателям. кому он считает нужным. Важнейшим моментом является факт, что только студент является единственным собственником своего ВЕБ-портфолио [3, 4].

Список используемых источников:

1. Крохин Е.Е. Как сделать портфолио для школьника? [Электронный ресурс], - http://womanadvice.ru/kak-sdelat-portfolio-dlya-shkolnika - Статья в интернете.
2. Панюкова С.В., Гостин А.М., Кулиева Г. А, Самохина Н.В. Создание и ведение веб-портфолио преподавателя. Методические рекомендации: учеб. пособие. – Рязань.: «Рязанский государственный радиотехнический университет», 2014 г. – 65 с.
3. Смоляр О.Б. Веб - портфолио в течение всей жизни. [Электронный ресурс], - https://proshkolu.ru/user/ovsey/blog/530440 - Статья в интернете.
4. Смоляр О.Б. Веб-портфолио длиною всю жизнь [Электронный ресурс], - https://infourok.ru/user/smolyar-ovsey-borisovich/material - Статья в интернете.

АНАЛИЗ МЕЖДУНАРОДНОГО ОПЫТА В СФЕРЕ ОБЕСПЕЧЕНИЯ ДОСТУПА ГРАЖДАН К СЕТИ ИНТЕРНЕТ

Игловский Валентин Дмитриевич

ОГБПОУ «Томский индустриальный техникум»

Руководитель: Бородин Алексей Юрьевич

Ни для кого не является секретом, насколько важную роль в развитии индивида и общества играет качественная и разнообразная информация. Распространение книгопечатания с последующей концентрацией результатов в библиотечные фонды, изобретение радио и охват сетями радиовещания всего земного шара – данные и подобные изобретения человеческой мысли сделали знания и информацию об окружающем мире всеобще доступной. Следующий ощутимый вклад в развитие общественного просвещения внес интернет, положив собой начало нового витка в развитие информационно открытого общества.

Для многих интернет стал альтернативной реальностью, точкой доступа, обеспечивающей доступ ко всем на текущий момент доступным человечеству знаниям и способной удовлетворить самые различные потребности, такие как, например, творческое самовыражение, общение и даже создание источников дохода. Однако, при всех его положительных сторонах, интернет имеет и отрицательные стороны. Он может являться источником социально-психологических угроз личности и приносить ощутимый ущерб различным организациям, в случае если они становятся жертвой киберпреступлений. Под предлогом борьбы с данными угрозами, различные государства видят необходимость вмешиваться в процесс развития интернета, используя различные, в том числе, и полулегальные средства. Данное вмешательство может быть обусловлено как искренними побуждениями, убежденностью в том, что необходимо защищать граждан собственной страны, так и потребностью руководства некоторых стран в защите собственных политических интересов.

Право граждан на информацию является одним из важнейших политических и личных прав человека и гражданина. Конституция Российской Федерации, принятая в 1993 году, в п. 4 ст. 29 устанавливает, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

В Европе и странах Запада интернет существует без ограничений, полностью доступный для каждого человека, не подвергается цензуре, люди имеют полную свободу действий. В таких странах как Канада уровень доступности интернета продолжал расти в 2016 году. Стоимость высокоскоростного доступа в Интернет остается низкой из-за большой конкуренции. Веб-сайты обычно не блокируются и не фильтруются. Незаконный контент может быть удален путем судебного разбирательства. Что касается удаления контента из-за нарушения авторских прав, в 2004 году Верховный суд Канады постановил, что интернет - провайдеры не несут ответственности за нарушения, совершенные их подписчиками. При этом Канада находится в первой десятке стран по индексу человеческого развития. В Канаде высокий уровень жизни и образование более доступно. Всему миру следует стремиться к таким показателям.

В России же 12 мая 2008 года появился Роскомнадзор, который по решению суда активно блокирует сайты по причине защиты детей от вредной информации, либо же борьбы с терроризмом, но так же очень много сайтов блокировалось необоснованно и без решения суда, количество которых превысило 4 млн. Для чего в России блокируются онлайн-библиотеки такие, как «Флибуста», это была бесплатная, свободная, некоммерческая онлайн-библиотека, позволявшая скачивать, читать, а также получать на электронную почту любые книги, имеющиеся в библиотеке? Не ограничение ли это наших прав и свободы, гарантированных Конституцией РФ?

Вероятно, что если так и продолжится, то интернет станет такой же ограниченный и контролируемый правительством, как в Китае. На территории КНР доступ к ряду иностранных сайтов ограничивается в рамках проекта «Золотой щит». Веб-страницы фильтруютсяпо ключевым словам, связанным с

государственной безопасностью, а также по «чёрному списку» адресов сайтов. Все иностранные поисковики в Китае фильтруют результаты поиска. В январе 2006 года компания «Google» открыла в Китае поисковый сайт на китайском языке, но по условию с правительством некоторые сайты должны были блокироваться из-за «политически некорректной информации». Также в Китае есть неофициально называемая «армия блогеров», которым платят за положительные высказывания о Китайской политике. Но несмотря на все это политическая активность в Китае есть, благодаря чему раскрывали коррупционную деятельность некоторых чиновников.

Но есть интернет и похуже чем, в Китае, например, в Северной Корее. На территории этой страны доступ к интернету имеют только ряд организаций, получивших для этого специальное разрешение. IP-адресов на 2013 год насчитывалось в 1200 – 1500. В основном доступом в интернет обладают лишь партийные деятели, пропагандисты, служба безопасности, предприятия, занимающиеся экспортом. В Северной Корее есть внутренняя сеть «Кванмён», полностью посвященная пропаганде, в этой сети была в основном информация научно-технического содержания, обновление информации на таких сайтах жестко контролируется правительством. В Корее разрешено использовать интернет иностранным фирмам и посольствам. А в феврале 2013 года был официально открыт доступ к 3G интернету, но был снова заблокирован через пару месяцев.

Так же есть и страны, не очень давно получившие доступ к интернету. Куба – страна, в которой интернет остается дефицитным и сейчас. Он очень дорогой, очень медленный, и пользоваться можно только в специальных местах (точках доступа). Первый интернет появился в Кубе в 2011 году, после прокладки кабеля из Венесуэлы, но им могли пользоваться только правительственные организации. Двумя годами позже по всей стране начали открываться интеренет-кафе, где интернет был весьма дорогой за час пользования. Мобильный интернет появился в Кубе в 2014 году, который работал только в специально отведенных для этого местах. В местах, отведенных для Wi-Fi

сети, есть много перекупщиков. Они покупают карточки для интернета и продают их пользователям в два раза дороже, чем предлагает поставщик. Услуги таких продавцов очень популярны, так как для покупки часовой карточки нужно было отстоять много часов. Так же при покупке карточки пользователь давал согласие в договоре, что он не будет использовать интернет для действий, которые могут рассматриваться как вредительские или предоставляющие угрозу для общественной информации.

По статистике интернет в большинстве стран частично свободный или несвободный вовсе. По сравнению с прошлыми годами доступность интернета увеличивается как в развитых странах, так и в странах, где интернет только появился или жестко контролируемый правительством. Канада по доступности интернета занимает 3-е место, а по индексу человеческого развития 9-е место. Россия же занимает 52-е место по доступности интернета и 50-е по индексу человеческого развития, не очень далеко от стран Азии и Ближнего Востока.

Список используемых источников:

1. [Электронный ресурс]. – Режим доступа:
2. https://ru.wikipedia.org/wiki
3. http://fishki.net/1769329-kak-vygljadit-internet-v-severnoj-koree.html
4. http://gtmarket.ru/ratings/freedom-on-the-net/info

ПРОФИЛАКТИКА БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ РАБОТЕ С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

Катков Максим Геннадьевич, Королева Анастасия Павловна, Финочка Елена Владимировна

ОГБПОУ «Томский техникум железнодорожного транспорта»

Руководители: Извекова Эльвира Орозбековна, Саиспаева Екатерина Дмитриевна

Работа включает в себя рассмотрение вопросов актуальности безопасности личности при работе с программным обеспечением различных цифровых устройств. В работе приведено исследование информационной осведомленности возрастной группы 16-20 лет по данному вопросу.

Введение:

Здесь мы Вам расскажем, что такое программа PRISM, расскажем шпионят ли за вами или нет, а если шпионят - кто, где и как. Как и при помощи какого программного обеспечения и оборудования за вами могут наблюдать. Кто раскрыл всем информацию что такое программа PRISM и для чего она предназначена. Существуют ли аналоги подобных программ в других странах и как от них укрыться или мы готовы с ними смерится, для обеспечения нашей безопасности.

Что такое программа PRISM ?

PRISM — государственная программа США, формально классифицированная как совершенно секретная, принятая американским Агентством национальной безопасности (АНБ) в 2007 году в качестве замены существующей на тот момент программе Terrorist Surveillance Program. [6]

6 июня 2013 года стало известно о существовании этой программы. Директор Национальной разведки США Клеппер подтвердил, что программа существует и работает в соответствии с законом об иностранной разведке.

Сведения, которые основаны на утечках документов, описывают программу как комплекс административных мер, которые дают возможность углубленного наблюдения за интернет-трафиком *некоторых* пользователей в

некоторых интернет ресурсов.

Как заявили спецслужбы, на сотрудничество пошли многие крупные нии, предоставив им доступ к серверам Microsoft (Hotmail, Skype), Facebook, и т.д. Но они отрицают причастность к системе и передачу данных о своих клиентах. Однако согласно документам, АНБ выплачивали миллионы долларов крупнейшим интернет-компаниям, связанных с программой слежки PRISM. Выплаты были осуществлены согласно решению суда (FISA), который признал, действия АНБ неконституционными в связи с тем, что программа слежки не могла разграничить иностранный трафик от внутреннего. Так виновны ли данные фирмы в данном инциденте или нет до сих пор неизвестно, однако российские чиновники обеспокоены причастностью данных фирм к данной программе.

Общеизвестный бывший агент американских спецслужб Джон Сноуден раскрыл информацию о программе PRISM, включающей в себя массовую слежку за переговорами американцев и иностранных граждан посредством телефона и Интернета. По его утверждениям, PRISM позволяет Агентству просматривать электронную почту, прослушивать голосовые и видеочаты, просматривать фотографии, видео, отслеживать пересылаемые файлы, узнавать другие подробности из социальных сетей.

Агентство Национальной безопасности потребовало открыть уголовное дело для расследования утечки информации о существовании PRISM в прессу.

Джастин Амаш (Justin Amash) от штата Мичиган, предложил поправку, которая должна ограничить полномочия АНБ по шпионажу: информация о телефонных разговорах и другие персональные данные будут собираться только у людей, которые задействованы в расследовании. Данная поправка могла бы стать важным шагом в борьбе с незаконной деятельностью АНБ. Но Белый Дом, в свою очередь, выступил с предложением отклонить поправку и разрабатывать другие методы для обеспечения безопасности нации без нарушения каких-либо законов.

Сноуден также разгласил сведения о существовании британской

программы слежения Tempora, и сообщил, что не пользуется iPhone из-за интегрированного программного обеспечения, позволяющего следить за пользователем.

Оказалось, что спецслужбы некоторых страны так же имеют подобные программы слежения. Как сообщило местное издание во Франции, Главное управление по внешней безопасности Франции (DGSE) собирает данные, передаваемые между компьютерами внутри страны, а также передаваемые и принимаемые из-за границы. По данным издания, слежка ведется за пользователями корпораций Google, Facebook, Apple и Yahoo!, а также за телефонными разговорами граждан.

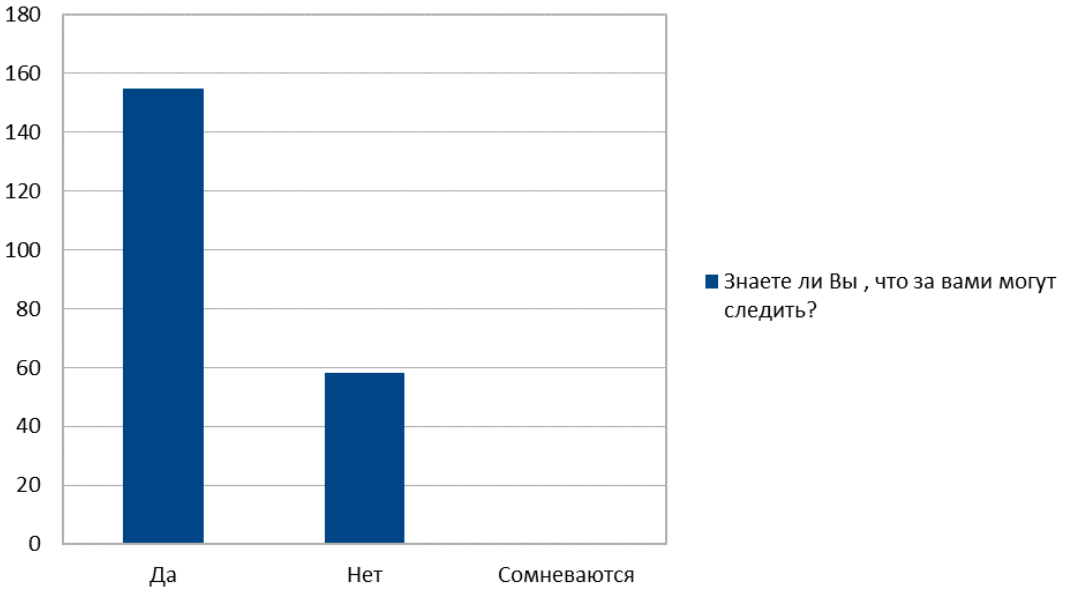
В Китае «Золотой щит», в Великобритании — Tempora, в Щвейцарии есть система «Оникс» она работает лучше чем PRISMA за с чёт того что собирает данные с телефона и других источников. В России есть аналог СОРМ-2. Впрочем, в отличие от американской, российская система ограничивается российскими телекоммуникационными сетями и российскими же пользователями.

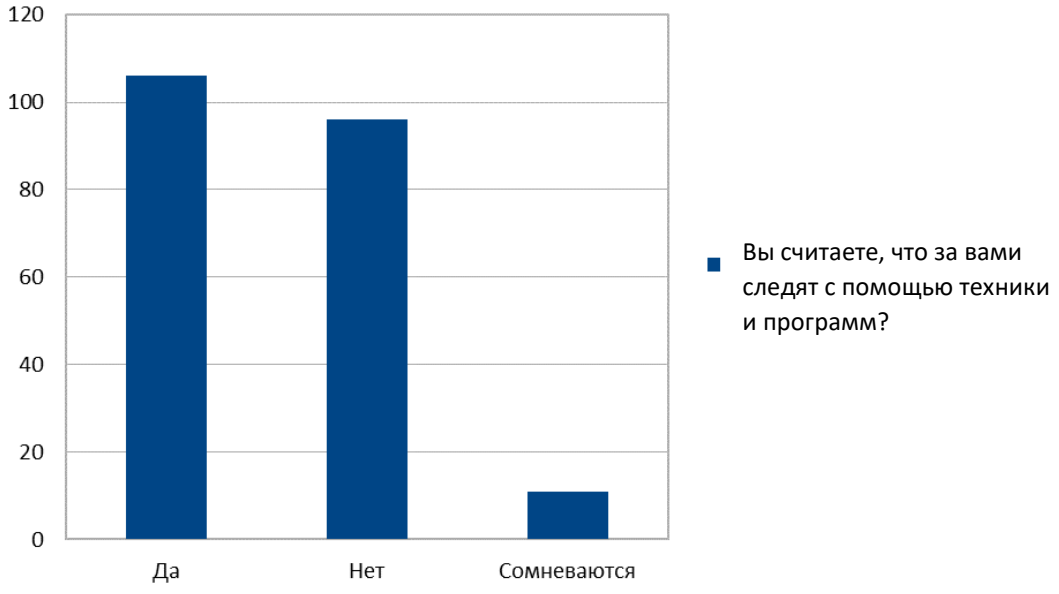
На сегодняшний день Россия обеспокоена безопасностью персональных данных своих граждан. По мнению отечественных чиновников зарубежные компании обязаны обеспечивать сохранность персональных данных россиян. Но готова ли Россия отказаться от программного обеспечения данных компаний, если этого потребует ситуация?

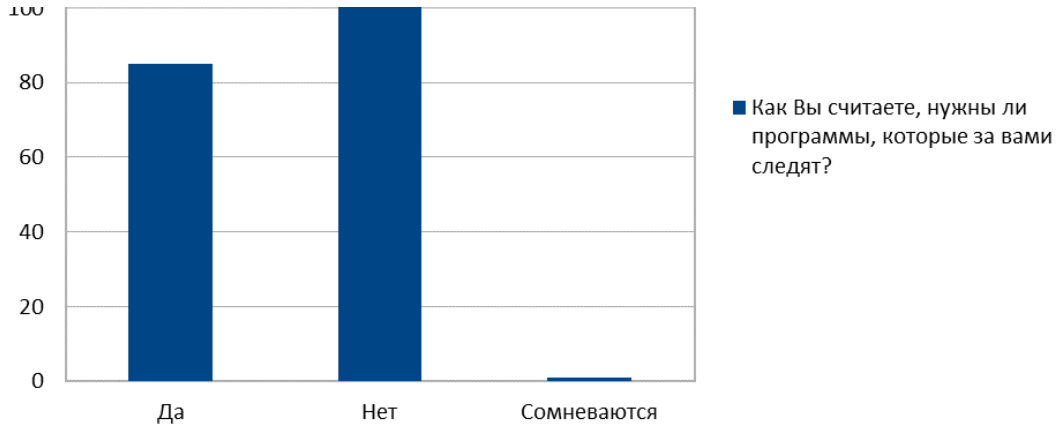
Согласно данным исследования экспертов Pew Research Center, несмотря на, казалось бы, всеобщее возмущение нарушением права на конфиденциальность личной жизни, оказалось, что 50% респондентов одобряют инициативу правительства.

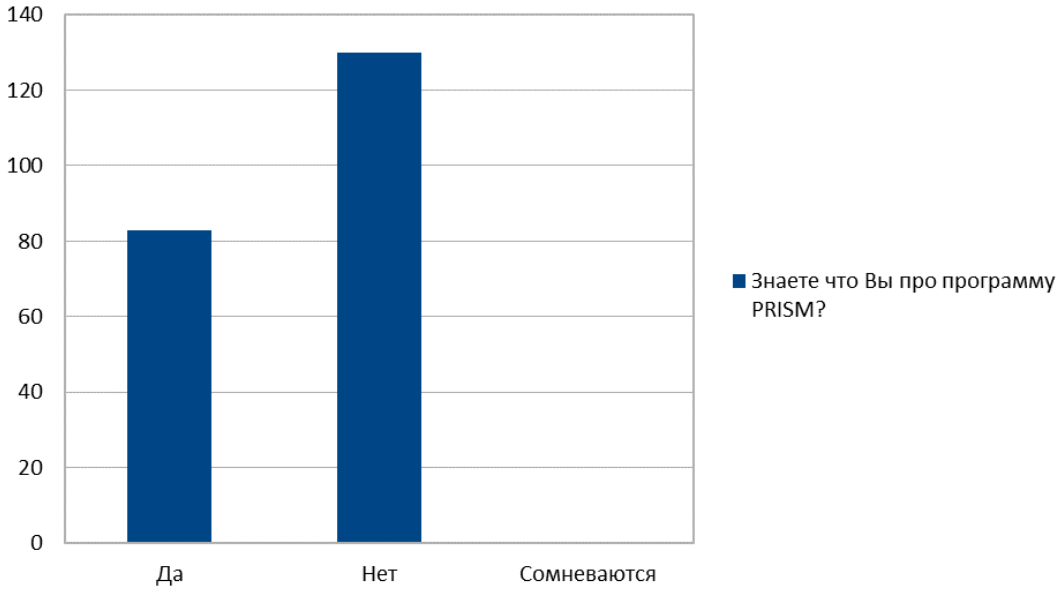
Результаты анкетирования

Мы провели исследование среди 1 (16-17 лет) и 4 (18-20 лет) курсов Томского техникума железнодорожного транспорта на понимание студентов о принципах сбора персональных данных посторонними людьми.









По данным анкетирования, респонденты предполагают, что за ними могут наблюдать, но не имеют полного представления о способах слежения, они не согласны с тем, что бы за ними следили, даже для обеспечения их собственной безопасности.

Заключение

В заключении хотелось бы сказать о возможных мерах, которые можно предпринимать, чтобы как можно больше оградить себя от слежки. Использовать профилактические мероприятия, проводимые пользователем своего ПК, быть в курсе того, что, используя любое устройство, за вами могут наблюдать и в соответствии с этим выстраивать свое поведение.

Список используемых источников:

1. Основы информационной безопасности [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В.Ю. Рогозин [и др.]. — Электрон. текстовые данные. — М.: ЮНИТИ-ДАНА, 2017. — 287 с. — 978-5-238-02857-6. — Режим доступа:

2. Галатенко В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. — Электрон. текстовые данные. — М.:

Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 266 с. — Режим доступа: http://www.iprbookshop.ru/52209.html

3. Рассолов И.М. Интернет-право [Электронный ресурс]: учебное пособие для студентов вузов, обучающихся по специальности 021100 «Юриспруденция» / И.М. Рассолов. — Электрон. текстовые данные. — М.: ЮНИТИ-ДАНА, 2012. — 143 с. — 5-238-00796-5. — Режим доступа:

4. Википедия, свободная энциклопедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/, свободный – (22.11.2017)
5. PRISM — недремлющее око или золотой клад?: https://habrahabr.ru/post/184680
6. Ларри Пейдж о программе PRISM: «What the...?»: https://habrahabr.ru/post/182554
7. https://www.securitylab.ru

ИСТОРИЧЕСКИЕ АСПЕКТЫ ВОЗНИКНОВЕНИЯ И РАЗВИТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДНР

Нека Валерия Сергеевна
МОУ «Школа № 45 г. Донецка»
ДНР
Руководитель: Адамова Светлана Евгеньевна

Введение

Мною выбрана актуальная тема «Исторические аспекты возникновения и развития информационной безопасности в ДНР». Сейчас информационная опасность - огромная проблема для человечества. Информационная безопасность – это состояние защищённости информационной среды, обеспечивающее её функционирование.

Мы постоянно имеем дело с компьютером и интернетом: общение, игры и развлечения, торговля, путешествия, медицина, образование. Всё это и еще многое другое составляет информационное пространство.

Функцией информационной безопасности является защита информации методами предупреждения и принятия соответствующих мер.

Молодое государство, становясь на ноги, ставит перед собой задачу не только раскрывать и доносить нужные факты до жителей республики, но еще и обезопасить ту информацию, которая имеет особый вес и секретность. Конечно, много интересного наверняка скрывается государством за ширмами секретности. Но населению хочется слышать всегда ту информацию, которая бывает не всегда приятная, но правдивая. Руководством республики приняты законы и правила подачи информации и обеспечения её безопасности. Определена терминология, касающаяся информационной безопасности.

Мною проработан достаточный объём литературы по этому вопросу. Надеюсь, что мне удалось осветить исторические аспекты возникновения информационной безопасности в ДНР, кратко рассмотреть пути решения проблем информационной безопасности.

1. Понятие информационной безопасности

Вопросы информационной безопасности можно увидеть в работах российских ученых – В.Н. Лопатина, Ю.С. Уфимцева, Е.А. Ерофеева, ряда зарубежных теоретиков – Д. Белла, У. Оуэнса.

Каким же опасностям подвергается информационная сфера?

1. Намеренные действия (кража, повреждение или удаление данных).
2. «Электронные» методы воздействия.
3. Компьютерные вирусы и другие вредоносные программы.
4. Спам.

«Естественные» угрозы: неправильное хранение, форс-мажорные обстоятельства. *Защита информации* – совокупность правовых, организационных, технических и других мероприятий, обеспечивающих сохранность, целостность информации и надлежащий порядок доступа к ней.

Таким образом, под *информационной безопасностью* понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или окружающей инфраструктуре.

2. Исторические аспекты возникновения и развития информационной безопасности в ДНР

По мнению Лопатина В. Н., категория «информационная безопасность» возникла с появлением средств связи между людьми. В развитии средств информационных коммуникаций он выделил несколько этапов:

I этап — до 1816 года — использование естественно возникавших средств связи.

II этап — начиная с 1816 года — начало использования электро- и радиосвязи.

III этап — начиная с 1935 года — появление радиолокационных и гидроакустических средств.

IV этап — начиная с 1946 года – изобретение ЭВМ.

V этап — начиная с 1965 года — создание локальных сетей.

VI этап — начиная с 1973 года — использование сверхмобильных коммуникационных устройств.

VII этап — начиная с 1985 года — создание глобальных сетей с использованием космоса.

VIII этап — начиная с 1998 года — подготовка и внедрение проекта международной концепции информационной безопасности.

В Донецкой Народной Республике информационной безопасностью занимаются с самого начала становления государства.

Утверждая права и свободы человека, гражданский мир и согласие, исходя из общепризнанных принципов равноправия и самоопределения народов, заявляя о стремлении обеспечить благополучие и процветание, Верховным Советом Донецкой Народной Республики принята ***Конституция*** Донецкой Народной Республики, протокол № 1 от 14 мая 2014 года. В ней в главе 2 «Защита прав и свобод человека и гражданина» в статье 16 сказано: п. 2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. В статье 17 этой же главы говорится, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

В статье 22 в п. 4 говорится, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, а в п.5 гарантируется свобода массовой информации.

Далее постановлением № 61-IНС Народного Совета ДНР от 19 июня 2015 года принят «***Закон о персональных данных***». Данным Законом регулируются отношения, связанные с обработкой персональных данных, с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях.

07.08.2015 г. постановлением № 71-IНС Народного Совета ДНР принят «***Закон об информации и информационных технологиях***». Данный Закон регулирует отношения, возникающие: при осуществлении права на все действия

с информацией; применении информационных технологий; обеспечении защиты. В Законе определены **принципы правового регулирования отношений в сфере защиты информации.**

В статье 14 в **пункте 1 «Государственное регулирование в сфере применения информационных технологий» сказано об** обеспечении информационной безопасности детей, Донецкой Народной Республики.

В пункте 3 статьи 14 так же отмечено, что при создании и эксплуатации государственных информационных систем, используемые в целях защиты информации методы и способы ее защиты должны соответствовать установленным требованиям.

В статье 23 **«Защита информации»** сказано, что защита информации представляет собой принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации, а так же указаны обязанности обладателей информации, операторов информационной системы.

В статье 24 **«Ответственность за правонарушения в сфере информации и информационных технологий» сказано, что л**ица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав.

Позднее, постановлением № 79-IHC Народного Совета от 2 октября 2015 года принят «***Закон о защите детей от информации, причиняющей вред их здоровью и развитию***».

Постановлением № 114-IHC Народного Совета от 11 марта 2016 года принят «***Закон о телекоммуникациях»*** в главе 1 которого сказано об обязанностях операторов телекоммуникаций, об ответственности за несанкционированный доступ к информации, передаваемой по телекоммуникационным сетям.

Как видим, правительством Донецкой Народной Республики с самого начала проводится кропотливая, последовательная работа по защите информации во всех областях её использования.

3. Пути решения проблемы информационной безопасности

Основными задачами информационной безопасности являются:

• обеспечение конфиденциальности информации;

• обеспечение целостности и достоверности информации;

• обеспечение юридической значимости информации;

• обеспечение доступности информации и информационных ресурсов.

Сегодня информационную безопасности обеспечивают:

1.Идентификация и аутентификация пользователей (комплекс 3А);

2. Шифрование информации, хранящейся на компьютерах и передаваемой по сетям;

3. Межсетевые экраны;

4. Виртуальные частные сети;

5. Контентная фильтрация;

6. Проверка целостности содержимого дисков;

7. Антивирусная защита;

8. Обнаружение уязвимостей сетей и анализаторы сетевых атак.

Каждый из вышеуказанных методов может быть использован как самостоятельно, так и в группе с другими.

Выводы

На основании прочитанной литературы, законодательных актов делаем вывод:

- информационная сфера ДНР играет ключевую роль в реализации многих конституционных прав и свобод граждан, в обеспечении возможности самореализации личности, духовном обновлении, политической и социальной стабильности общества, обеспечении функционирования государства;

- информационная сфера становится все более важным фактором развития экономики.

Нормальная жизнедеятельность человеческого общества все в большей степени зависит от состояния информационной сферы. Защита национальных интересов, реализуемых в информационной сфере, от опасностей внешнего и внутреннего характера составляет основное содержание деятельности по обеспечению информационной безопасности ДНР.

Информационная безопасность – это состояние защищённости жизненно-важных интересов личности, общества, организации, предприятия от потенциально и реально существующих угроз.

Список используемой литературы и интернет- ресурсов:

1. Конституция Донецкой Народной Республики
2. Закон Донецкой Народной Республики о персональных данных
3. Закон Донецкой Народной Республики об информации и информационных технологиях
4. Закон Донецкой Народной Республики о защите детей от информации, причиняющей вред их здоровью и развитию
5. Закон Донецкой Народной Республики о телекоммуникациях
6. Манойло А.В., Петренко А.И., Фролов Д.Б.. Государственная информационная политика в условиях информационно-психологических конфликтов высокой интенсивности и социальной опасности: Учебное пособие. М.: МИФИ. - 392 с.. 2004
7. Лопатин В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества. М.: 2000. – 428 с;
8. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. − М.: Книжный мир, 2009. – 352 с.

ЖИЗНЬ БЕЗ АНТИВИРУСА

Смокотин Лев Алексеевич

ОГБПОУ «Томский политехнический техникум»

Руководитель: Пирогова Светлана Ивановна

Большинство пользователей используют антивирусную защиту. Задавшись вопросом, возможно ли использование ПК без антивирусной программы, я решил проверить это на собственном опыте. Для этого я переустановил на собственном компьютере операционную систему с форматированием жесткого диска, не устанавливая антивирус.

Далее я активно, но разумно пользовался интернетом: скачивал фильмы, сериалы, музыку, игры, программы. Использовал как официальные ресурсы, так и торрент-трекер. Через шесть месяцев объем содержимого составил 675 GB без учёта того, что было удалено за ненадобностью. Чистка корневых директорий всех логических дисков и облачных хранилищ на предмет неизвестных файлов проводилась в ручном режиме. Производились оплаты различных услуг через бановскую карту и электронные кошельки, такие как Яндекс.Деньги,Qiwi и PayPal. Все транзакции проходили успешно и никакой подозрительной активности я не заметил.

По окончании эксперимента я установил самый эффективный из бесплатных антивирусов, по мнению большинства IT- сайтов, просмотренных мною. Сразу после установки отобразилось уведомление об угрозе безопасности в лице svchost.com, находящемся в папке windows. Обращаю внимание, что файл повторяет название svchost.exe - главный процесс для служб, загружаемых из динамических библиотек в системе Windows. Я провел полное сканирование компьютера, оставив это предупреждение без внимания. Антивирус отсканировал **274930** файлов, из них **701** были отмечены как представляющие угрозу. Это составило **0,26 %**от всех файлов - ничтожно малый процент зараженности. Оказалось, все заражённые файлы имеют расширение .exe, и заражены они старым белорусским вирусом Neshta, написанным на Delphi. В папке windows была совершена подмена оригинального процесса svchost.exe

на тело вируса svchost.com, а в реестре была создана запись, которая присваивала ему обязанность запускать файлы с расширением exe и msi.

На данном этапе я прибегнул к математической статистике.

Каков процент заражения вирусом Neshta по отношению к другим вирусам и каков шанс был подхватить именно этот вирус?

Используем сведения об угрозах, обнаруженных с использованием лечащей утилиты Dr.Web CureIt! Вероятность подхватить именно Neshta всего P(A)=0.78

Neshta – вирус, который не уйдет из ПК без ваших усилий. Относительно безопасный, т.к. не крадет ваши данные и пароли, но проблемный и трудноудаляемый.

Далее нужно было избавится от вируса Neshta.

Я решил удалить запись реестра, чтобы предотвратить запуск вируса при включении любой программы. Однако, каждый файл ~~формата~~ расширения exe набрал в объеме **41472** байта, в котором хранился скрипт восстановления записи реестра в случае его изменения. Выходит, любое изменение реестра не приносило никакого эффекта, т.к. даже при включении компьютера фоновые процессы работы windows с вредоносным скриптом внутри снова назначали тело вируса как исполнительный файл при открытии программ. Избавиться от вируса данными манипуляциями не удалось.

Можно ли полностью избавиться от заражения? Теоретически можно. Большинство программ можно вылечить, но некоторые исполнительные процессы, на которых зиждется работа операционной системы, рядовому пользователю вылечить не представляется возможным, т.к. для этого нужен 2-й компьютер + специальный софт или загрузочный накопитель + навыки работы с BIOS. Для избавления от вируса я прибегнул к переустановке ОС с форматированием всех логических томов, т.к. я и планировал сделать в конце эксперимента.

Заключение:

Даже при наличии антивирусной защиты полная безопасность компьютера не гарантирована. От некоторых угроз без критических решений избавиться практически невозможно.

Поэтому необходимо либо создать антивирус, который сможет вылечить заражение в активном режиме работы ПК, либо обезопасить интернет на уровне сервера. Тогда отпадёт необходимость пользоваться антивирусным ПО каждому отдельному пользователю.

Таким образом, проанализировав вредоносные последствия незащищенной системы с постоянным подключением к всемирной паутине, мы приходим к выводу:

Компьютер без антивируса находится в крайней опасности, т.к. даже такой «старый» вирус как Neshta может заблокировать большинство программ и даже такие меры предосторожности, как резервное копирование могут не помочь. Поэтому антивирус для ПК – обязателен.

СПОСОБЫ БОРЬБЫ С РАЗМЕЩЕННЫМ В СЕТИ ИНТЕРНЕТ ОСКОРБЛЕНИЕМ В СВОЙ АДРЕС

Смолкина Олеся Григорьевна

ОГБПОУ «Томский индустриальный техникум»

Руководитель: Маслова Екатерина Константиновна

Введение

Свободный доступ к всемирной сети и возможность общения с любыми пользователями интернета зачастую сопровождается свободой выражений, моральные рамки которых ограничиваются особенностями воспитания. Порою пользователь сети сталкивается с такой проблемой, как оскорбления в свой адрес, размещенные другими лицами. Подобные действия наказуемы по закону, в этом случае действует статья за оскорбление личности в социальных сетях, на различных форумах и интернет-сайтах, которые позволяют получать обратную связь от пользователей в виде комментариев и вопросов. Из этого вытекает *проблема данной работы*: как с юридической точки зрения противостоять подобным оскорблениям.

Актуальность выбранной темы определяется необходимостью изучения наказания оскорбительного поведения во всемирной паутине, поскольку распространение интернет-сети давно вышло за рамки личного пользования. Я решила проанализировать законы, защищающие личность каждого отдельного гражданина, которые накладывают ответственность за неподобающее поведение не только при реальном общении, но и посредством различных средств коммуникации, включая социальные сети.

Методологическую базу исследования составили общенаучные методы познания, включающие принцип объективности, системности, индукции, дедукции и др. Наряду с общенаучными методами познания применялись частнонаучные методы: описательный, лингвистический, сравнительно-правовой.

Историография по данной теме не слишком обширна. Данная проблема исследована Дмитрием Чернокальцевым. Этот юрист работает в сфере информационных технологий, автор многих статей на данную тему, знает толк в своем деле и в решениях этих непростых задач. В его работах очень подробно описано, как бороться с данной проблемой, как искать способы борьбы с аморальными личностями в интернете. Он один из немногих, кто помогает бороться и защищать честь и достоинство в социальных паутинах.

В сборнике «Управление в социальных и экономических системах», включающем материалы международной научно-практической конференции под редакцией Ю.С. Руденко, Р.М. Кубовой, М.А. Зайцева, есть материалы секции 5 «Правовые проблемы защиты чести, достоинства и деловой репутации в интернете», где собраны статьи по данной проблеме, например, указанная в списке литературы статья Л. А. Мишиной [3.].

А также с зашитой нашей репутации в социальных сетях нам помогают научные статьи, размещенные в сети интернет, где очень подробно описано, как можно бороться за свои права, и какое наказание ждет обидчика. Например, статья К. Муромцевой [4.].

1. Способы борьбы с точки зрения закона

Свободный доступ к всемирной сети и возможность общения с любыми пользователями интернета зачастую сопровождается свободой выражений, моральные рамки которых ограничиваются особенностями воспитания. Порою пользователь сети сталкивается с такой проблемой, как оскорбления в свой адрес, размещенные другими лицами. Подобные действия наказуемы по закону, в этом случае действует статья за оскорбление личности в социальных сетях, на различных форумах и интернет-сайтах, которые позволяют получать обратную связь от пользователей в виде комментариев и вопросов.

Столкнувшись с высказываниями оскорбительного содержания в социальных сетях, пользователь, порой не знает о том, как защититься от нападок

со стороны недоброжелателей. Следует помнить, что закон защищает личность каждого отдельного гражданина и накладывает ответственность за неподобающее поведение не только при реальном общении, но и посредством различных средств коммуникации, включая социальные сети.

К оскорблениям, преследуемым по закону, относятся не только слова, произнесенные обидчиком в действительности, но и выражения, зафиксированные в письменном или печатном виде. При условии, если удалось определить обидчика и доказать его действия, можно привлечь его к ответственности, административной или уголовной, в зависимости от тяжести формы и категории адресанта. Практика применения законодательства в отношении нанесения оскорблений в социальных сетях ранее отсылала к ст. 130 УК, комментарий к которой указывает не только на объективную, но и на субъективную сторону преступления, регламентирует ее как целенаправленное намерение. По субъективной стороне оскорбление отлично от хулиганства тем, что оскорбление вызвано личным неприязненным отношением обидчика к потерпевшему, а мотив хулиганства больше направлен на проявление озорства и неуважительного отношения к обществу. Субъектом преступления, связанного с оскорблением, может являться гражданин, который признан вменяемым и достиг возраста 16 лет [1.]. Однако в настоящее время этот регламент устарел. Пользователь социальной сети, допустивший в адрес другого гражданина оскорбительные высказывания, должен знать, что подобные действия будут расценены как нарушение, а к обидчику будет применена мера наказания на основании положений ст. 5.61 Кодекс РФ об Административных правонарушениях (КоАП), введена Федеральным законом от 07.12.2011 N 420-ФЗ):

1. Оскорбление, то есть унижение чести и достоинства другого лица, выраженное в неприличной форме, – влечет наложение административного штрафа на граждан в размере от одной тысячи до трех тысяч рублей; на должностных лиц – от десяти тысяч до тридцати тысяч рублей; на юридических лиц – от пятидесяти тысяч до ста тысяч рублей.

2. Оскорбление, содержащееся в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, – влечет наложение административного штрафа на граждан в размере от трех тысяч до пяти тысяч рублей; на должностных лиц – от тридцати тысяч до пятидесяти тысяч рублей; на юридических лиц – от ста тысяч до пятисот тысяч рублей.

3. Непринятие мер к недопущению оскорбления в публично демонстрирующемся произведении или средствах массовой информации – влечет наложение административного штрафа на должностных лиц в размере от десяти тысяч до тридцати тысяч рублей; на юридических лиц – от тридцати тысяч до пятидесяти тысяч рублей [2.].

Таким образом, изменения в законодательстве привели к тому, что оскорбление в подавляющем большинстве случаев было переквалифицировано на административное правонарушение.

Формы нанесения оскорблений в социальных сетях могут быть разными. К публичным оскорблениям относятся следующие формы выражений:

1. Реплики неприличного содержания, с бранью и ненормативной лексикой, высказанные в адрес конкретного человека.
2. Фотографии и иные виды передачи информации, опубликованные без согласия гражданина с целью компрометации.
3. Размещение оскорбительных высказываний на общедоступных форумах, в разделах для комментирования. Для того, чтобы иметь основания привлечь обидчика к ответственности, текст оскорбительного содержания должен быть размещен в открытом публичном доступе.

Отличие подобных оскорблений от клеветы существенно. С позиции применения наказаний клевета регламентируется Уголовным Кодексом, а ответственность за оскорбление будет определена по конкретным обстоятельствам и степени тяжести проступка. Закон предусматривает уголовное или ад-

министративное наказание при рассмотрении дела об оскорблениях в социальных сетях. Чаще ненормативные и негативные высказывания рассматриваются в рамках административных правонарушений с применением КоАП. В ряде случаев обидчику грозит реальный тюремный срок, если объектом оскорблений стал военнослужащий или должностное лицо. Если в рамках административной ответственности наказание будет ограничено 1-3 тысячами рублей, то при оскорблении военнослужащего согласно ч.2 ст. 130 УК может быть назначен тюремный срок сроком до одного года.

2. Трудности применения закона

В отличие от других форм оскорблений высказывание в социальной сети трудно отследить. Нужно найти свидетелей, готовых подтвердить факт отправки унизительных реплик в адрес потерпевшего. Выполнить это практически нереально. Другой проблемой является невозможность полной идентификации человека, в адрес которого поступали негативные высказывания. Таким образом, унизительные слова, сказанные обобщенно, без точного указания адресанта, не могут расцениваться как оскорбления конкретного гражданина. Если аккаунт не дает исключительно точного описания человека, в адрес которого были написаны оскорбительные слова, наказание за нанесение оскорблений не может быть применено. Если было принято решение наказать обидчика по закону, нужно подать заявление в мировой суд. Сложность обвинения состоит в том, что получатель оскорбляющих слов должен самостоятельно обеспечить доказательство факта правонарушения, в то время, как в рамках уголовного судопроизводства данная обязанность падает на следователя.

3. Порядок привлечения к ответственности

Следующие действия помогут определить порядок наказания при оскорблениях, наносимых в соцсетях: создание файла со скриншотом экрана компьютера, на котором фиксируется обидное для истца высказывание. Тре-

буется заверить подлинность данного скриншота у нотариуса. Скриншот должен быть выполнен таким образом, чтобы можно было доказать факт правонарушения и определенность высказывания. Потребуется установить личность человека, опубликовавшего нелицеприятную запись, и представить доказательства совершения им данного нарушения. Составляется заявление о нанесении оскорбления. Заявление передается в отдел полиции. Если заявитель намерен получить компенсацию за моральный ущерб, иск подается в участок мирового суда. Заявление для мирового суда должно содержать все детали происшедшего, к нему прикладывают документальные доказательства действий нарушителя.

Наказание обидчика в рамках законодательства допускается при соблюдении следующих условий:

1. Возраст обидчика превышает 16 лет.
2. Полное доказательство вины прилагаемыми документами
3. Предварительно было проведено досудебное урегулирование.

Каждый человек должен знать, как пожаловаться на оскорбления в интернете, т.к. это позволит наказать обидчика законным способом и даже получить причитающуюся компенсацию. При этом важно помнить, что данные законы в нашей стране достаточно молодые, из-за чего добиться положительного решения в суде очень непросто. Привлечь к ответственности по данному нарушению довольно сложно, поэтому исков с просьбой наказать виновных в оскорблениях очень мало. Еще меньше доля исков, которые были удовлетворены судом.

Заключение

Проанализировав литературу по данной теме, я пришла к выводу, что, несмотря на то, что факт оскорбления налицо, достаточно сложно добиться справедливости и наказания обидчика через суд. Все дело в том, что многие пользователи регистрируются под различными вымышленными именами и установить, кто конкретно выступил обидчиком, довольно сложно. В отличие от других форм оскорблений, высказывание в социальной сети трудно отследить. Нужно найти свидетелей, готовых подтвердить факт отправки унизительных реплик в адрес потерпевшего. Выполнить это практически нереально.

Другой проблемой является невозможность полной идентификации человека, в адрес которого поступали негативные высказывания. Таким образом, унизительные слова, сказанные обобщенно, без точного указания адресанта, не могут расцениваться как оскорбления конкретного гражданина. Если аккаунт не дает исключительно точного описания человека, в адрес которого были написаны оскорбительные слова, наказание за нанесение оскорблений не может быть применено.

Если было принято решение наказать обидчика по закону, нужно подать заявление в мировой суд. Сложность обвинения состоит в том, что получатель оскорбляющих слов должен самостоятельно обеспечить доказательство факта правонарушения, в то время, как в рамках уголовного судопроизводства данная обязанность падает на следователя.

В результате работы, можно сделать следующие выводы:

1. Оскорбления в соцсетях пока редко приводят к судебным искам или заявлениям в полицию. Однако не исключается, что со временем это станет обычным делом.
2. У многих людей культура общения, в том числе виртуального, находится на очень низком уровне.
3. Можно ожидать, что со временем нормы онлайн-поведения будут

контролироваться гораздо строже, чем сейчас.

Список используемых источников:

1. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 28.04.2015 г.) // Собрание законодательства РФ. 1996. № 25. Ст. 130.

2.Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 30 декабря 2001 г. N 195-ФЗ (по состоянию на 1 января 2014г.). М.: Юрист, 2014.

3. Мишина Л. А. Удаление и опровержение информации в сети Интернет / Л. А. Мишина, А. И. Миронова // Управление в социальных и экономических системах. – 2015. – С. 545 –552.

4. Муромцева К. Ст. 130 УК РФ. Оскорбление личности [Электронный ресурс]. – Проект «SYL.ru», 2013-2017. – Режим доступа: https://www.syl.ru/article/305557/st-uk-rf-oskorblenie-lichnosti (дата обращения 20.11.17).

5. Публичное оскорбление в интернете: кто виноват и что делать? [Электронный ресурс]. – Новости информационных технологий, 2010-2017. – Режим доступа: http://www.pvsm.ru/zakon/38497 (дата обращения 20.11.17).

6. Чернокальцев Д. Клевета и оскорбления в сети Интернет: надо защищаться! [Электронный ресурс]. – Правовая социальная сеть для юристов. ООО "Редакция журнала "ЗАКОН", 2010 - 2017. – Режим доступа: https://zakon.ru/blog/2014/4/9/kleveta_i_oskorbleniya_v_seti_internet_nado_zashhishhatsya (дата обращения 20.11.17).

ЗАКОНОДАТЕЛЬНОЕ РЕГУЛИРОВАНИЕ ПРАВА ГРАЖДАН НА ИНФОРМАЦИЮ

Шаршавина Ирина Вячеславовна
ОГБПОУ «Томский политехнический техникум»
Руководитель: Рязанова Галина Михайловна

Введение

Право граждан на информацию является одним из важнейших политических и личных прав человека и гражданина. Конституция Российской Федерации, принятая в 1993 году, в п.4 ст.29 устанавливает, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, за исключением перечня сведений, составляющих государственную тайну, определяется законом.

В соответствии с Федеральным законом "Об информации, информатизации и защите информации" от 25 января 1995г.// СЗ РФ с.47. пользователи - граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения - обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцами этих ресурсов необходимость получения запрашиваемой ими информации. Исключение составляет информация с ограниченным доступом, содержащая государственную, коммерческую или иную специально охраняемую законом тайну или конфиденциальную информацию.

Законом охраняется информация, содержащая:

- государственную тайну - ст. 29 Конституции РФ, Закон РФ "О государственной тайне". Перечень конкретных сведений, составляющих государственную тайну, утвержден указом Президента РФ № 61 от 24 января 1998 г.;
- коммерческую и служебную тайну - ст. 139 ГК, ст. 185 УК.

Признание тех или иных сведений конфиденциальными является прерогативой правообладателя. Перечень таких сведений содержится в Указе

Президента РФ от 6 марта 1997 № 188 "Об утверждении перечня конфиденциального характера" ФЗ "Об утверждении перечня конфиденциального характера" от 6 марта 1997г. № 188// СЗ РФ с.133.

Закон охраняет:

- банковскую тайну и тайну денежных вкладов - ст. 185 УК, ст. 26 Закона РФ "О банках и банковской деятельности" ФЗ "О банках и банковской деятельности" // ст. 857 ГК, ст. 857 ГК;
- тайну усыновления - ст. 155 УК, ст. 159 Семейного кодекса;
- адвокатскую тайну - ст. 137 УК, ч. 7 ст. 51 УПК;
- нотариальную тайну - ст. 175 УК, ч. 2 ст. 16 «Основ законодательства РФ о нотариате»;

Передача конфиденциальной информации в правоохранительные органы и судебные органы осуществляется в строго установленном порядке, т.е. по официальным мотивированным письменным запросам в связи с возбужденным уголовным делом или проведением проверки в порядке ст. 109 УПК РФ.

1. Понятие права граждан на информацию

1.1 Основные информационные права и свободы, основания их ограничения

Среди национальных интересов России особое место занимает реализация основных прав и свобод граждан в информационной сфере. Она основывается на принципах свободы информации и запретительном принципе права (все, что не запрещено законом, разрешено). Этот принцип закреплен в основных международных правовых документах, Конституции Российской Федерации и ряде других законов.

"Основным объектом правоотношений здесь выступает право на информацию, а субъектами являются любые физические и юридические лица.

Как записано во Всеобщей декларации прав человека, утвержденной и провозглашенной Генеральной Ассамблеей ООН 10 декабря 1948 г., каждый человек имеет право на свободу (ст. 3), право на свободу мысли (ст. 18); право

на свободу убеждений и на свободное выражение их" Бачило И.Л. « О праве на информацию в Российской Федерации». М., 1997. - с. 217-220.

Это право включает свободу беспрепятственно придерживаться своих убеждений и свободно искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ (ст. 19).

Позднее эти права и свободы нашли отражение в ряде международных документов:

-в ст. 19 Международного пакта о гражданских и политических правах (вступил в силу 23 марта 1976 г.), где уточняется, что эти свободы относятся ко всякого рода информации, идеям и способам их распространения;

-в ст. 13 Декларации прав и свобод человека и гражданина (принята Верховным Советом РСФСР 22 ноября 1991 г.), где в дополнение к перечисленным правам провозглашена свобода слова «Декларация прав человека и гражданина»

Эти права и свободы также закреплены в Конституции Российской Федерации (принятой всенародным голосованием 12 декабря 1993 г.):

-право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени - ч. 1 ст. 23;

- право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений - ч. 2 ст. 23 и многих других документах.

2. Правовое регулирование права на информацию

2.1 Законодательное регулирование права на информацию в России

"Проблема права на информацию чрезвычайно важна, прежде всего, в плане практического его применения. Однако исследование процесса включения этого права человека и гражданина в систему национального и международного права ставит вопросы, касающиеся жизни и эволюции его как юридической категории; места, связей и взаимосвязей в системе других прав человека; понимания содержания и механизмов его реализации" Бачило И.Л., Лопатин В.И., Федотов М.А. Информационное право: Учебник /Под ред. акад.

Б.Н. Топорнина - СПб.: Издательство "Юридический центр Пресс", 2001 г. - с. 220.

В полном объеме право на информацию было зафиксировано конституционно после принятия Декларации прав и свобод человека и гражданина Верховным Советом РСФСР в 1991 г. и включения этого текста в Конституцию 1992 г. Ныне действующая Конституция Российской Федерации 1993 г. содержит специальную норму о праве на информацию (ч. 4 ст. 29 Конституции РФ).

Федерального закона РФ о праве на информацию граждан в силу ряда обстоятельств нет, хотя проекты на этот счет есть. Однако законодатель и разработчики этих проектов до сих пор не выработали единых позиций по ряду основных вопросов о точности ориентации на виды субъектов, о содержании права на информацию.

Не будет преувеличением утверждать, что реализация права граждан на информацию, обеспечение свободного доступа к имеющей общественное значение информации, информационная открытость органов власти являются важнейшими условиями и критериями функционирования правового государства. Именно реализация права граждан на информацию обеспечивает реальное, а не только формальное участие граждан в жизни государства.

Следует подчеркнуть особую значимость этого права: оно выступает связующим элементом всей системы основных прав и свобод. Только при условии его соблюдения можно говорить о фактической реализации личных, политических, социальных, экономических, экологических и культурных прав и свобод.

Сегодня в России не существует единого нормативно-правового акта, который бы создавал механизм реализации права граждан на информацию, прописанный выше. Нормы, закрепляющие право на доступ к информации и порядок такого доступа, можно сказать, разбросаны по всему законодательству Российской Федерации.

Так, в 1993 году был издан Указ Президента РФ N 2334 "О дополнительных гарантиях прав граждан на информацию", провозгласивший принцип информационной открытости деятельности государственных органов, организаций и предприятий, общественных объединений, должностных лиц.

Этот документ был принят исходя из того, что право на информацию является одним из фундаментальных прав человека, определяется стремление к расширению реальных возможностей граждан и их объединений активно участвовать в управлении государственными и общественными делами, содействовать развитию местного самоуправления.

Закон о праве граждан на информацию призван обеспечить получение гражданином информации, необходимой прежде всего для реализации всех его прав и свобод, для удовлетворения всех его жизненно важных интересов. Гражданин имеет право на получение, производство и распространение информационного продукта, который он сам создает или приобретает за свои средства. Он может заниматься и предпринимательством в области информации и информатизации без образования юридического лица, если это не запрещено законом. Всё это свидетельствует о приоритете правового регулирования права граждан на информацию.

В связи с остротой проблемы информационного обеспечения органов государственной власти важно обратить внимание на меры, принимаемые по подготовке проектов программ, связанных с упорядочением правовой информации (с правовой информатизацией) в системе органов исполнительной власти, с информатизацией органов государственной власти субъектов РФ. В этом направлении в последнее время работа оживилась. Тема права на правовую информацию и другие наиболее важные массивы информационного ресурса, необходимые для поднятия правовой и социальной культуры населения, гарантий получения знаний и воспитания человека должна быть отражена и в законе о праве на информацию.

2.2 Конституция РФ о праве на поиск, получение и передачу информации. Правовые гарантии

В ч. 4 ст. 29 Конституции РФ сформулирована основополагающая норма информационного права на доступ к информации: "Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом".

Следует отметить, что многие конституционные права и возможность их реализации непосредственно связаны с информационными правами граждан. Так, в соответствии с ч. 1 ст. 37 Конституции РФ "каждый имеет право свободно распоряжаться своими способностями к труду, выбирать род деятельности и профессию". Но для того чтобы реализовать это право, необходимо владеть информацией, касающейся характера и специфики той или иной профессии. В ч. 1 ст. 41 Конституции установлено право каждого на охрану здоровья и медицинскую помощь. Но только при наличии информации о том, куда следует обратиться, каким образом выбрать врача, можно полностью его реализовать. В ч. 3 той же статьи устанавливается ответственность должностных лиц за сокрытие фактов, создающих угрозу для жизни и здоровья людей.

Один из основных вопросов в реализации права на информацию - возможность доступа к ней.

"Для обеспечения информационных прав индивидуальных и коллективных субъектов органы государственной власти согласно Конституции РФ обязаны опубликовывать законы и иные нормативные акты, затрагивающие права, свободы и обязанности человека (ч. 3 ст. 15 Конституции РФ); обеспечивать каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими права и свободы лица» (ч. 2 ст. 24).

В ст. 24 Конституции РФ указаны органы, которые обязаны "обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом". Это органы государственной власти, органы местного самоуправления, их должностные лица. Основным законом прямо не предусмот-

рены возможности и основания получения необходимых документов в отношении отдельных видов информации (экологической, медицинской и т.п.), но они нашли свое отражение в законодательных и подзаконных актах.

Информационное обеспечение территории и отдельных ее структур наряду с упорядочением потоков информации требует создания территориальной информационной системы и банков данных, располагающих оперативными сведениями о проживающем на данной территории населении, о зарегистрированных юридических лицах, данные земельного кадастра и т.д. Обязанности по информированию субъектов информационного права помимо Конституции содержатся в ряде законов: Федеральном Конституционном законе "О чрезвычайном положении", Законе РФ "О безопасности", Законе РФ "О занятости населения в Российской Федерации".

Таким образом, мною были обозначены основные положения конституционного права граждан на информацию, а также основные проблемы данного института.

Заключение

Подводя итоги данной работы, следует еще раз сказать, что права граждан на информацию сравнительно молодой институт права, который относится к такому разделу Конституционного права, как права и свободы человека. В условиях современного общества информация стала являться важнейшей ценностью, что потребовало немедленной законодательной регламентации общественных отношений, связанных с поиском, получением, распространением, передачей информации. В Российской Федерации основным гарантом данного права выступила Конституция, которая закрепляет данное право в статье 29. Данная статья является обобщающей для всех остальных конституционных норм, связанных с правом граждан на информацию. Как уже говорилось, существует множество законов и иных нормативно-правовых актов, которые затрагивают данный институт права. Это еще раз говорит о важности данного правового института для развития общественных отношений в условиях построения правового демократического государства.

По моему мнению, нужно создать хотя бы один централизованный правовой акт, способный улучшить бы регламентацию общественных отношений касательно данного правового института. Конечно же говоря о свободе информации следует подразумевать, что даже в демократическом обществе есть определенные рамки этой свободы.

Необходимо разработать концепцию системы нормативно-правового регулирования права граждан на информацию и обеспечения информационной открытости власти. Развивая систему законодательного обеспечения права граждан на информацию, необходимо принять федеральный закон, осуществляющий регулирование доступа граждан к персональным данным о себе и обеспечить сохранность этих данных от других пользователей.

Список используемых источников:

1. Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 г.) .

2. Закон РФ "О государственной тайне" от 21 июля 1993 г. \\ СЗ РФ. № 41. Ст. 4673

3. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

4. Постановление Правительства РФ от 12 февраля 2003 г. № 183 "Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти"

5. Агапов А.Б. Основы федерального информационного права России. М.: "Юристъ", 1995 г.- 321 с.

6. Информационно-правовой портал «Гарант. Ру» http://www.garant

7. Студенческая библиотека-онлайн. Право граждан на информацию. http://studbooks.net/2391286/pravo/pravo_grazhdan_informatsiyu

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И СРЕДСТВА ЗАШИТЫ ИНФОРМАЦИИ

Мещеринов Игорь Сергеевич, Никитин Вадим Витальевич

Республиканский многопрофильный лицей-интернат при ДонНУ

г. Донецк, ДНР

Руководитель: Гридина Валерия Валериевна

Актуальность. В информационную эру безопасность общества жизненно необходима, поэтому один из признаков высокоразвитой страны - максимально возможная безопасность информации. Но, несмотря на все попытки государства защитить общество, всё же существует ряд механизмов, способных обойти эту защиту. Ещё с начала человеческой истории была необходимость в передаче и хранении информации, и в наши дни физическое воздействие на общество заменилось на информационное. В 21 веке основной упор в обеспечении безопасности делается на электронные носители информации. Но, несмотря на все попытки защитить информационное пространство общества, удаётся это далеко не всегда. С увеличением роста потребности в применении персональных компьютеров в жизни обыкновенных пользователей и увеличением объёма хранимой информации возросло и количество не только всевозможных программ-вирусов, препятствующих нормальной работе персональных компьютеров, но и, например, дезинформации от СМИ и прочих источников информирования общества. И потому информационная безопасность личности – фундаментальная проблема. Без её решения невозможен ответ на вызовы XXI века. Для предотвращения информационных атак существуют специальные средства защиты информации, которые используются почти во всех областях человеческой деятельности. Этот факт говорит о том, что тема актуальна в настоящее время.

Целью исследования является рассмотрение основных методов, средств создания систем защиты безопасности.

Информационная безопасность государства — состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере.

В современном социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью.

Для надёжной защиты информации недостаточно простых механизмов защиты требуется создание целого ряда средств, направленных на обеспечение информационной безопасности. Условно их можно разделить на два типа:

1. Формальные
2. Неформальные

Формальные средства защиты - средства защиты, которые выполняют свою функцию без непосредственного вмешательства человека. К формальным средствам относятся: технические, физические, программные и аппаратурные.

Неформальные средства защиты - средства защиты, которые зависят от деятельности и выполняют свою функцию при непосредственном вмешательстве человека. К неформальным средствам относятся: законодательные и организационные.

Методика защиты информации устанавливает совокупность мероприятий по её защите от возможного взлома, несанкционированного доступа и различного рода воздействий, которые могут повредить или заблокировать информацию. Её задачами являются:

- защита информации от уничтожения (следует учитывать также природное и техногенное воздействие;

- обеспечение безопасности каналам передачи и защита от потери информации;

- защита конфиденциальных данных пользователей.

Основные методы защиты информации можно разделить на несколько типов:

- препятствие;

- механизмы шифрования;

- регламентация;

- принуждение;

- побуждение.

Препятствие – физическое противодействие злоумышленнику.

Механизмы шифрования – один из наиболее распространённых методов защиты информации, применяемый не только при обработке, но и при хранении информации на физических накопителях. Представляет из себя криптографическое закрытие информации.

Регламентация – метод автоматизированной обработки, передачи и использования информации, при котором возможность получения доступа к информации сведена до минимума.

Принуждение – метод защиты, при котором пользователи и персонал вынуждены соблюдать регламентированные правила обращения с информацией под угрозой уголовной и материальной ответственности.

Побуждение – такой метод, который побуждает пользователя и персонал соблюдать моральные и этические нормы, запрещающие разрушать установленные правила.

Данные методы и средства успешно применяются на практике за счёт их различных свойств, в том числе морально-эстетических норм и административных средств.

В обстоятельствах нынешней России угрозы информационной безопасности личности можно было бы разделить на 3 группы.

К первой группе можно отнести угрозы, которые относятся к развитию девиантного поведения личности. В результате сумбурности, в особенности в нынешних СМИ, мы сталкиваемся с такими явлениями как: агрессивность среди молодёжи, резкая активация иррациональной сферы общественного сознания; усиление садомазохистских наклонностей в поведении молодых людей и т.д.

Ко второй группе относятся угрозы, которые связаны с вестернизацией граждан РФ, занимающих позицию той части российского истеблишмента, которой близки монетаристские взгляды, но и глобальной тенденцией в политике США к навязыванию собственных ценностей в мире как наиболее истинных. А также повсеместной унификацией и универсализацией.

А к третьей группе относятся угрозы, которые связанные нарушением социальной преемственности поколений. В наши дни отчуждение общества от позитивного исторического опыта - один из основных принципов построения информационных потоков в современных СМИ.

Как можно заметить, для России характерен рост численности населения, использующего Интернет. А это явление сопровождается включением значительного числа населения в сферу интеллектуального труда, развитием интеллектуальной собственности, появлением новых информационных технологий, а всё это не может просто так пройти мимо человеческой личности.

Наше время интересно тем, что созданные глобальные информационные системы охватывают миллионы человек по всему миру. Наиболее масштабной и известной всем является сеть Интернет, объединяющая более 2 млрд пользователей.

Вывод. Таким образом с каждым днём количество угроз и средств защиты против них растёт в геометрической прогрессии, что ещё раз доказывает значение информации в современном обществе.

Список литературы

1. Информационная безопасность личности. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-lichnosti (дата обращения: 19.11.2017).
2. Методы и средства защиты информации. [Электронный ресурс]. URL: http://life-prog.ru/1_4145_metodi-i-sredstva-zashchiti-informatsii.html (дата обращения: 21.11.2017)
3. Виды и источники угроз информационной безопасности. [Электронный ресурс]. URL: http://infoprotect.net/note/vidyi_i_istochniki_ugroz_informacionnoy_bezopasnosti (дата обращения: 21.11.2017)
4. Средства защиты информации от несанкционированного доступа. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/sredstva-zaschity-informatsii-ot-nesanktsionirovannogo-dostupa (дата обращения: 22.11.2017)

СЕКЦИЯ 4. «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В ПЛАКАТАХ»

Воронов Кирилл Максимович

ОГБПОУ «Томский экономико-промышленный колледж»

Руководитель: Крыжановская Анна Павловна

Видякина Ирина Андреевна

ОГБПОУ «Томский индустриальный техникум»

Руководители: Мазенина Александра Николаевна,
Рыжиков Павел Александрович

Зубарева Кристина Игоревна

ОГБПОУ «Томский экономико-промышленный колледж»

Руководитель: Крыжановская Анна Павловна

Богданова Марина Андреевна

ОГБПОУ «Томский политехнический техникум»

Руководитель: Рязанова Галина Михайловна

Киреев Дмитрий Юрьевич
ОГБПОУ «Томский политехнический техникум»
Руководитель: Пирогова Светлана Ивановна

Лунев Алексей Юрьевич
ОГБПОУ «Томский политехнический техникум»
Руководитель: Пирогова Светлана Ивановна

Бородина Марина Юрьевна

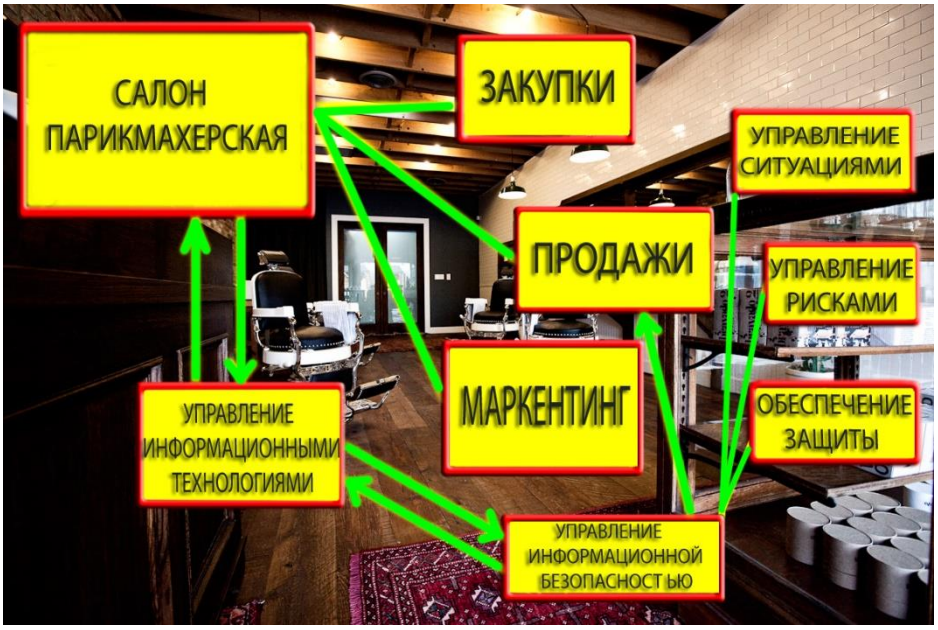
Гимназия №55 им. Е. Г. Версткиной, г. Томск

Руководитель: Бжитских Елена Владимировна

Веремеев Роман Андреевич

ОГБПОУ «Колледж индустрии питания, торговли и сферы услуг»

Руководитель: Лукьянова Наталья Петровна



Гайдамак Анастасия Сергеевна

ОГБПОУ «Асиновский техникум промышленной индустрии и сервиса»

Руководитель: Зиновьев Вячеслав Юрьевич

Глухов Кирилл Геннадьевич

ОГБПОУ «Томский техникум информационных технологий»

Руководитель: Кабикова Алина Владимировна

Грачев Михаил Леонидович

МОУ «Школа №11 г. Тореза», ДНР

Руководитель: Любченко Наталья Юрьевна

Дергачев Захар Васильевич

ОГБПОУ «Томский Техникум Информационных Технологий»

Руководитель: Кабикова Алина Владимировна

Загребин Герман Сергеевич
ОГБПОУ «Томский техникум информационных технологий»
Руководитель: Ненашева Алла Ивановна

Зотин Сергей Константинович
ОГБПОУ «Томский индустриальный техникум»
Руководитель: Асадулина Галия Спартаковна

Лисовский Вадим Витальевич

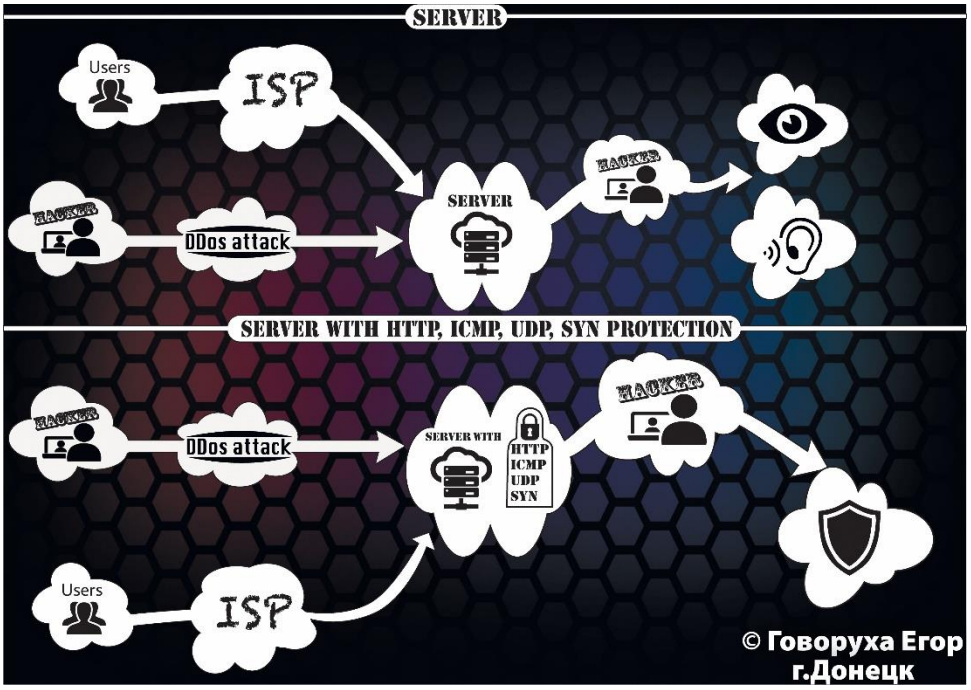
МОУ «Школа №11 г. Тореза», ДНР

Руководитель: Любченко Наталья Юрьевна

Говоруха Егор Андреевич

Республиканский многопрофильный лицей-интернат при ДонНУ, г. Донецк, ДНР

Руководитель: Гридина Валерия Валериевна



Решетник Никита Сергеевич
ОГБПОУ «Томский техникум информационных технологий»
Руководитель: Кабикова Алина Владимировна

Сидиков Ильяс Даниярович
ОГБПОУ «Томский техникум информационных технологий»
Руководитель: Кабикова Алина Владимировна

Соколова Марина Александровна, Шатохина Алена Дмитриевна
ОГБПОУ «Томский техникум информационных технологий»
Руководитель: Веснова Елена Евгеньевна

Сухаревский Максим Евгеньевич

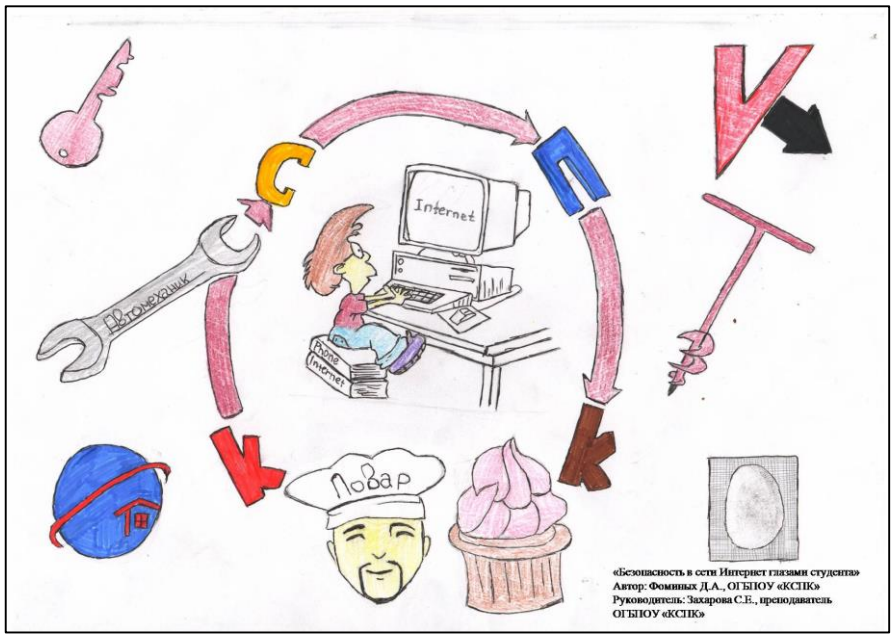
ОГБПОУ «Колпашевский социально - промышленный колледж»

Руководитель: Криницкая Наталья Александровна

Фоминых Данила Александрович

ОГБПОУ «Колпашевский социально - промышленный колледж»

Руководитель: Захарова Светлана Евгеньевна



«Безопасность в сети Интернет глазами студента»
Автор: Фоминых Д.А., ОГБПОУ «КСПК»
Руководитель: Захарова С.Е., преподаватель ОГБПОУ «КСПК»